VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zotavení po havárii poštovních služeb na bázi Microsoft Exchange

Disaster recovery of mail services based on Microsoft Exchange

2012 Lenka Kučerová

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání diplomové práce

Student: **Bc. Lenka Kučerová**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T025 Informatika a výpočetní technika

Téma: Zotavení po havárii poštovních služeb na bázi Microsoft Exchange
Disaster Recovery of Mail Services Based on Microsoft Exchange

Zásady pro vypracování:

Cílem práce bude prostudování oblasti obnovy poštovní infrastruktyry a na základě těchto informací vytvoření analýzy rizik a scénářů obnovy dat na platformě Microsoft Exchange. Tyto scenáře budou následně otestovány a navrhnuty i případné optimalizace.

1. Seznamte se s postupy pro obnovu systému a dat po havárii poštovních služeb a popište, jak je toto řešeno v rámci procesů ITIL.
2. Seznamte se a popište jaké možnosti v tomto ohledu nabízí poštovní služba MS Exchange.
3. Na modelovém příkladě společnosti popište aktuální stav a proveďte analýzu rizik této společnosti.
4. Vytvořte scénář řízené obnovy poštovního systému po havárii v této modelové společnosti.
5. Daný scénář otestujte a navrhněte případné optimalizace poštovního prostředí společnosti.

Seznam doporučené odborné literatury:

Podle pokynů vedoucího diplomové práce.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Lumír Návrat**

Datum zadání: 18.11.2011
Datum odevzdání: 04.05.2012

doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně. Uvedla jsem všechny literární prameny a publikace, ze kterých jsem čerpala.

V Ostravě 22. dubna 2012 ..... Kučerová .....

Poděkování náleží především vedoucímu diplomové práce Ing. Lumírovi Návratovi za metodické vedení, vstřícný přístup, konstruktivní náměty a cenné rady v průběhu zpracování této práce.

Dále děkuji svým dětem, rodině a přátelům, za duševní podporu a trpělivost.

Abstrakt

Diplomová práce popisuje obnovu systému po havárii poštovních služeb.

První část popisuje metodiku ITIL a její doporučení pro řízení kontinuity služeb v rámci životního cyklu ITSCM. Následně jsou zachycené možnosti obnovy poštovních služeb na bázi Microsoft Exchange.

Praktická část je zasazena do společnosti s implementovaným poštovním systémem MS Exchange 2007. V této modelové společnosti je provedena analýza rizik a pro kritická rizika jsou navržená protiopatření. Na základě analýzy jsou vypracované scénáře obnovy.

Na závěr jsou všechny scénáře obnovy poštovního systému otestovány v připraveném prostředí.

Klíčová slova: zotavení po havárii, ITIL, Exchange, hodnocení rizik, scénáře obnovy

Abstract

This diploma thesis describes disaster recovery of an e-mail system after failure.

First part is dedicated to ITIL methodology and its recommendations for Service Continuity Management in context of ITSCM lifecycle, supplemented by description of e-mail service recovery that is based on Microsoft Exchange product.

Second, practical part is set in the model company that implemented Microsoft Exchange 2007. Risk analysis is conducted there and needed countermeasures are proposed for the highest risks. Analysis is used as a basis for composing Recovery Scenarios.

All scenarios from second part are tested in lab environment in the final part of this thesis.

Keywords: disaster recovery, ITIL, Exchange, risk assessment, recovery scenarios

Seznam použitých zkratek a symbolů

AD	–	Active Directory
BC	–	Business Continuity
BCP	–	Business Continuity Planning
BE	–	Backup Exec
BIA	–	Business Impact Analysis
CAS	–	Client Access Server, serverová role MS Exchange Serveru
CCR	–	Cluster Continuous Replication
CCTA	–	Central Communications and Telecommunications Agency
DAG	–	Database Availability Group
DC	–	Domain Controller
DR	–	Disaster Recovery
DRP	–	Disaster Recovery Planning
Edge	–	Edge Transport, serverová role MS Exchange Serveru
EXIN	–	Examination Institute for Information Science
GC	–	Global Catalog
HA	–	High Availability
Hub	–	Hub Transport, serverová role MS Exchange Serveru
ISEB	–	Information Systems Examination Board
ITIL	–	Information Technology Infrastructure Library
ITRP	–	IT Recovery Plans
ITSCM	–	IT Service Continuity Management
ITSCP	–	IT Service Continuity Plans
ITSMF	–	IT Service Management Forum
LCR	–	Local Continuous Replications
MBX	–	Mailbox, serverová role MS Exchange Serveru
NLB	–	Network Load Balancing
OGC	–	Office of Government Commerce
RPO	–	Recovery Point Objective
RSG	–	Recovery Storage Group
RTO	–	Recovery Time Objective
SCR	–	Standby Continuous Replications
SG	–	Storage Group
UM	–	Unified Messaging

Obsah

Seznam tabulek

Seznam obrázků

1 Úvod

Elektronická pošta, jako prostředek komunikace, je používána drtivou většinou společností. V souladu s charakterem podnikání, vyspělosti konkrétní společnosti a s podnikovými procesy, kterých se elektronická pošta účastní, nabývá význam poštovní služby klíčových nebo pouze podpůrných hodnot.

Klíčové hodnoty vykazují procesy, které jsou nezbytné k zajištění chodu či dosažení obchodních cílů společnosti. Podpůrné hodnoty představují procesy, jenž poskytují služby základním procesům a nemají přímý vliv na činnost podnikání.

Poštovní služby jsou úzce spjaty s informačními systémy a firemními aplikacemi, jejichž dostupnost a spolehlivost je pro řadu společností klíčová, tj. má přímý vliv na kontinuitu podnikání - Business Continuity (BC). Je zřejmé, že význam poštovních služeb nezávisí primárně na velikosti společnosti, nýbrž na hodnotě samotné elektronické komunikace pro určitou společnost.

V zájmu každé společnosti je udržet kritické služby funkční v nepřetržitém provozu a v požadované kvalitě po celou stanovenou dobu. Také servisní údržba se plánuje tak, aby dodávka služby (využívání emailového systému) nebyla poznamenána snížením kvality či dokonce přerušením, případně aby tento čas byl co nejkratší.

Ve snaze maximálně zmírnit negativní dopady běžných servisních a očekávaných výpadků se navrhují systémy s vysokou dostupností - High Availability (HA). Implementují se řešení na bázi clusteru či lépe geoclusteru, replikační mechanismy a zálohovací systémy dostupné v samotných aplikacích, využívá se nabízených řešení třetích stran, příp. služeb společností poskytující IT outsourcing nebo cloud computing.

Ovšem i přes veškeré úsilí architektů IT infrastruktury může dojít k výpadkům mnohem závažnějšího rázu a tedy i rozsahu vzniklých škod. Mezi možné příčiny se řadí hardwarový výpadek datového centra, živelná katastrofa, infekční epidemie, lidský úmysl atp. V této souvislosti hovoříme o havárii systému a následně o zotavení služeb – Disaster Recovery (DR).

Rozdíl mezi High Availability a Disaster Recovery spočívá především v závažnosti příčin, které HA a DR v rámci svých plánu řeší a v dopadu potenciálních škod na kontinuitu podnikání. HA zpravidla dosáhneme navýšením zdrojů a uzpůsobením IT infrastruktury, zatímco u DR se vypořádáváme s nedostupnosti zdrojů, což může vážně ohrozit kontinuitu podnikání.

Jelikož obojí (HA a DR) mohou za jistých okolností využívat stejné scénáře nebo se vzájemně podporovat a doplňovat, je přínosné vytvářet plány obnovy po havárii již ve

fázi návrhu podnikové infrastruktury společně s konceptem služby vysoké dostupnosti. Dále se budu zabývat zotavením poštovních služeb po havárii MS Exchange tedy DR.

1.1 Zotavení po havárii

Pojmy Disaster recovery, Zotavení po havárii a Katastrofický scénář shodně označují v oblasti IT proces obnovy po havárii. Předmětem obnovy jsou služby kritické pro zajištění kontinuity podnikání. Pořadí obnovy služeb závisí na stanovené prioritě služby a je definováno při sestavování plánu obnovy.

Plánování obnovy Disaster Recovery Planning (DRP) je součástí plánů kontinuity podnikání Business Continuity Planning (BCP) a vytváří se společně s návrhem systému. V této fázi je však vytváření plánů obnovy mnohdy podceňováno a odsouvá se, ve snaze vyhnout se nutným zvýšeným nákladům na potřebné zdroje a zároveň urychlit proces návrhu systému, na pozdější období.

Pokud scénář DR není vytvořen ani dodatečně, vystavuje společnost rizikům nejen sebe, ale také své zákazníky, kteří mohou být na jejím provozu závislí. Případná katastrofa pak sebou nese časové prodlevy v dodávce služeb, finanční ztráty přímé nebo v podobě náhrad škod způsobených zákazníkům a také může zapříčinit poškození dobrého jména společnosti.

V kontextu vyspělosti společnosti z pohledu plánování disaster recovery je definována uživatelskou skupinou SHARE a společnosti IBM stupnice o 7, resp. 8 vrstvách.

VRSTVA 0
No off-site data, společnost nemá žádná zálohovaná data ani záložní hardware.

VRSTVA 1
Data backup with no Hot Site , společnost má implementované zálohovací řešení s úložištěm dat ve stejné lokalitě.

VRSTVA 2
Data backup with a Hot Site , společnost má implementované zálohovací řešení s úložištěm dat v záložní lokalitě.

VRSTVA 3
Electronic vaulting , zálohovací řešení s úložištěm dat v záložní lokalitě, využívá se logického oddělení kritických dat a jejich duplicitního zálohování na rychle dostupné úložiště. Plán obnovy umožní prioritní obnovení kritických dat.

VRSTVA 4
Point-in-time copies , zálohovací řešení s centrálním úložištěm na hardwarových diskových polí - FlashCopy, Storage Area Network.

VRSTVA 5
Transaction integrity, řešení na bázi produkční a záložní lokality, zálohovací zařízení je pouze v produkční lokalitě, umožňuje zálohování, archivaci a obnovu vybraných dat.

VRSTVA 6
Zero or little data loss, zálohovací zařízení je umístěno v každé z lokalit, lokality jsou navzájem plně zastupitelné, řešení umožňuje zálohování vybraných dat, duplikaci produkčních a záložních komponent

VRSTVA 7
Highly automated,business-integrated solution, řešení na bázi duplikace a integrace dat mezi rovnocennými lokalitami s podporou automatického převzetí služeb.

Z výše uvedené stupnice lze snadno vyrozumět závislost implementovaného řešení zálohování na zabezpečení před možnými typy havárie a tedy i schopnosti včasné obnovy kritických služeb a procesů. Sestavování plánu obnovy je pro každou společnost zcela individuální záležitostí.

Plán DR nelze zobecnit, jelikož jakákoli možná příčina vzniku rizika představuje pro každou společnost jinou úroveň ohrožení. Proto není účelem ve všech společnostech implementovat DRP na 7.vrstvě stupnice, ale mít kvalitně zpracovaný scénář DR, který v maximální možné míře snižuje rizika kontinuity podnikání konkrétní společnosti.

V současné době nabízí řada IT společností své služby a poradenství v oblasti BCP a DRP. Služby zahrnují zpravidla analýzu rizik podnikové infrastruktury, vyhodnocení rizik a výběr vhodných opatření, příp. poskytnutí kompletního řešení zvládání rizik, tj. včetně poskytnutí úložišť, implementace zálohovacích systémů, archivačních mechanismů a služeb souvisejících s obnovou systému.

K významným společnostem, které se zabývají problematikou DR patří HP, IBM, San guard a ICM.

2 Obnova systému a dat po havárii poštovních služeb

Postupy pro obnovu systému a dat po havárii se začali vyvíjet v 70 letech 20.století jako nutnost zabezpečit IT systémy před nežádoucími výpadky. Potřeba zajistit bezchybný a nepřetržitý provoz měla v té době význam především pro vládní instituce, obranné složky a vědeckou sféru. Nejlepší praktiky a doporučení vycházející z osvědčených postupů řízení IT v organizaci jsou obsaženy v souhrnu publikací - Information Technology Infrastructure Library (ITIL).

Plánování kontinuity podnikání a zotavení po havárii nutně spadá do rámce řízení IT a kromě doporučení ITIL je také řízeno řadou vydaných národních norem a mezinárodních standardů.

Mezinárodní standardy
ISO/IEC 20000 - Information technology - Service management
ISO/IEC 27001 - Information technology - Security techniques - Information security management systems
ISO/PAS 22399 - Societal security - Guideline for incident preparedness and operational continuity management
ISO/IEC 24762- Information technology - Security techniques - Guidelines for information and communications technology disaster recovery services
ISO 31000 – Risk management - Principles and guidelines

Národní normy
BS 15000 - British Standard for IT Service Management
BS 25777 / PAS 57 - IT Service Continuity Management
BS 25999 / PAS 56 - Business Continuity Management. Code of Practice & Specification
AS/NZS 4360 - Australian/New Zealand Standard for Standard in Risk Management
AS/NZS 5050 - Business continuity - Managing disruption-related risk

2.1 Information Technology Infrastructure Library

Dříve než se zaměřím na doporučené postupy pro obnovu systému a dat v rámci procesů ITIL, připomenu význam ITIL, motivaci vzniku a vývoj jednotlivých verzí. V současné době je nejrozšířenější řadou publikací ITILv3, jehož aktualizace z července 2011 je vydávána pod názvem ITIL 2011.

ITIL® je veřejně dostupný rámec, jenž popisuje nejlepší praktiky ve Správě služeb IT. Poskytuje rámec pro zvládnutí IT v organizaci, pojednává komplexně o službách a zaměřuje se na neustálé měření a zlepšování kvality dodávaných služeb IT, a to jak z pohledu businessu, tak z pohledu zákazníka. Toto zaměření je hlavní příčinou celosvětového úspěchu ITIL® a přispělo k rozšířenému využití a ke klíčovým přínosům, získaným u těch orga-

nizací, které aplikovaly tyto techniky a procesy ve svých strukturách.

Některými z těchto přínosů jsou:

- Správa financí (Financial management)
- zvýšená spokojenost uživatelů a zákazníků se službami IT
- zlepšená dostupnost služeb, což přímo vede ke zvýšeným ziskům a obratu businessu
- finanční úspory plynoucí ze snížení opakovaných prací, ztraceného času, zlepšené správy a využití zdrojů
- zkrácení času pro uvedení nových produktů a služeb na trh
- zlepšení podkladů pro rozhodování a optimalizace rizik. [3]

ITIL vznikl jako požadavek vlády Spojeného království Velké Británie a Severního Irska na zavedení kvalitativního standardu informačních technologií a zvýšení efektivity poskytování služeb IT. Zpracováním byla pověřena agentura Central Communications and Telecommunications Agency (CCTA). Hlavním cílem zamýšleného standardu bylo zajištění vysoké kvality poskytovaných služeb IT, snížení nákladů, optimalizace zdrojů, zvýšení výkonu, zajištění vysoké dostupnosti a škálovatelnosti systému, dále schopnost měření výkonnosti IT procesů a řízení rizik.

ITILv1
Po několikaletém zpracovávání informací, provádění analýz a vytváření efektivních metodik byly výsledky shrnuty do 31 knih pokrývajících veškeré aspekty poskytování IT služeb. Soubor knih se dále rozrostl a v letech 1989-1995 vydala společnost CCTA, dnes Office of Government Commerce (OGC), celkem 41 publikací knihovny ITIL v1.

Obsáhlost knihovny ITIL v1 odráží ucelený konspekt metodiky pro efektivní poskytování IT služeb a to především zabezpečení dodávky služeb z pohledu stability infrastruktury IT. Hlavní procesy představuje Service Support a Service Delivery, přičemž každá disciplína jmenovaných procesů byla zachycena v samostatné knize. Nebylo výjimkou, že v publikacích docházelo k opakovanému zaznamenávání shodných metod popsaných v jinak nezávislých celcích.

Příklady titulů disciplín ITILv1 : Planning and Control for IT Services, A Guide to Business Continuity Management, Unattended Operating, Human Factor in the Office Environment, Office Design and Planning, Fire Precautions in IT Installations, Management of Electrical Interference, Secure Power Supplies, Specification and Management of a Cable Infrastructure, Management of Acoustic Noise.

ITILv2
Z důvodu obtíženého praktického využití byla metodika ITILv1 revidována, redundantní informace odstraněny a publikace byly r 2001 nahrazeny novou verzí o 8 knihách, které tvoří souhrn nejlepších praktik a doporučení. Hlavní procesy Service Support a Service

Delivery zůstaly zachovány a jejich disciplíny jsou souhrnně popsány vždy v jedné knize. Další knihy zachycují provozní pokyny k oblastem ICT Infrastructure Management , Application Management , Security a knihy pro podporu praktické implementace The Business Perspective , Planning to Implement Service Management , ITIL® Small-scale Implementation.

Na přípravě druhé verze, zaměřené především na kvalitu a efektivitu IT procesů, se kromě OGC podíleli také experti soukromých subjektů participujících v neziskovém sdružení IT Service Management Forum (ITSMF).

Verze č.2 ovlivnila změny britské normy BS 15000 a stala se základem pro mezinárodní normu ISO/IEC 20000. To patrně způsobilo, že se na ITIL začalo nahlížet jako na uznávaný standard řízení a správy služeb IT, přestože se jedná pouze o souhrn doporučení nejlepších technik. Význam ITIL umocňuje rovněž možnost certifikace odborné způsobilosti IT Service Management (ITSM) pro jednotlivce u některé z mezinárodně uznávaných certifikačních autorit Information System Examination Board (ISEB) nebo Examination Institute for Information Science (EXIN).

ITILv3
Se vzrůstajícím počtem společností, které zavádí řídící procesy dle doporučení ITIL ve svých IT strukturách, roste také množství připomínek ke stávající verzi. Připomínkuje se zejména nedostatečná škálovatelnost a neschopnost aplikovat ITIL na životní cyklus služby, přicházejí požadavky na jasné vymezení pojmů, doplnění ITIL o příklady, šablony, procesní model, atd.

Množství připomínek a požadavků bylo zpracováno a v roce 2007 je uveřejněna nová verze ITIL v3.

Hlavní část tvoří 5 knih, které pokrývají životní cyklus služby : Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement. Šestá kniha The Official Introduction to the ITIL – Service Lifecycle je oficiálním úvodem do ITIL nové struktury v podobě životního cyklu služby.

Hlavní procesy v jednotlivých publikacích

Strategie služeb (Service Strategy)
- Správa financí (Financial management)
- Správa portfolia služeb (Service Portfolio Management - SPM)
- Správa požadavků (Demand Management)

Návrh služeb (Service Design)
- Správa katalogu služeb (Service Catalogue Management - SCM)
- Správa úrovní služeb (Service Level Management - SLM)
- Správa kapacit (Capacity management)
- Správa dostupnosti (Availability Management)
- Správa kontinuity služeb IT (IT Service Continuity Management - ITSCM)
- Správa bezpečnosti informací (Information Security Management - ISM)
- Správa dodavatelů (Supplier Management)

Přechod služeb (Service Transition)
- Správa změn (Change Management)
- Správa aktiv a konfigurace (Service Asset and Configuration Management - SACM)
- Správa znalostí (Knowledge management - KM)
- Plánování a podpora přechodu (Transition Planning and Support)
- Správa releasů a rozmísťování (Release and Deployment Management)
- Ověření a testování služby (Service Validation and Testing)
- Vyhodnocení (Evaluation)

Provoz služeb (Service Operation)
- Správa událostí (Event Management)
- Správa incidentů (Incident Management)
- Provádění požadavků (Request Fulfillment)
- Správa přístupů (Access Management)
- Správa problémů (Problem Management)

Průběžné zlepšování služeb (Continual Service Improvement)
- Zlepšování služeb (Service Improvement)
- Měření služby (Service Measurement)
- Vykazování služeb (Service Reporting)

Pro účely obnovy systému a dat se zaměříme na publikaci Service Design a proces zachycený v části Správa kontinuity služeb IT.

2.2 IT Service Continuity Management

IT Service Continuity Management (ITSCM) podporuje veškeré procesy kontinuity podnikání zajištěním možnosti obnovy všech nutných technických a servisních zařízení v požadované kvalitě a sjednaném časovém horizontu. Předmětem obnovy jsou dodávky služeb počítačových systémů, aplikací, datových úložišť, počítačových i telekomunikačních sítí, technické podpory a činnost Service Desku, jediného kontaktního místa pro zprostředkování komunikace mezi uživatelem a poskytovatelem IT služby.

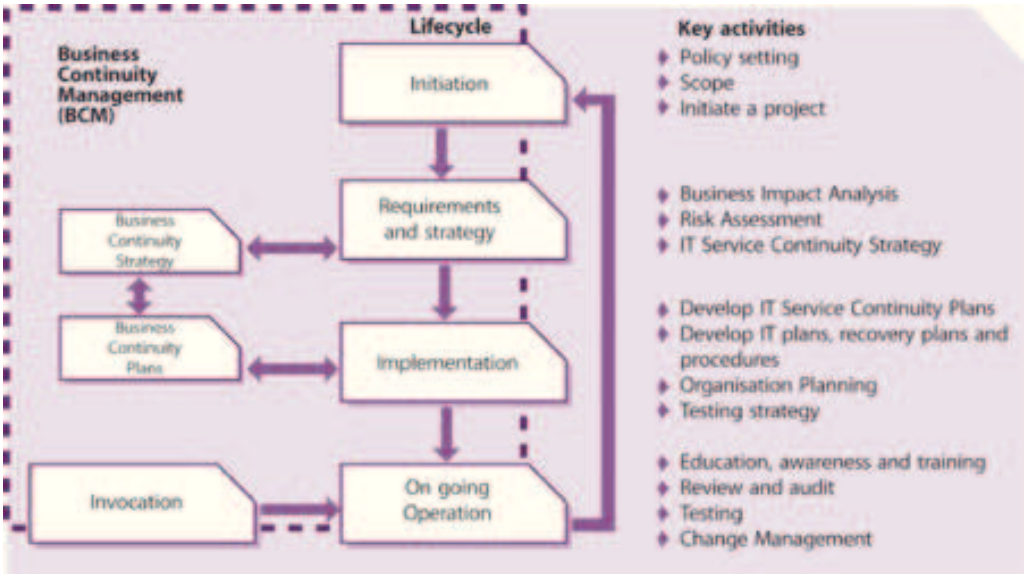
ITSCM je základní součást většiny podnikových procesů, jenž jsou kritické pro kontinuitu podnikání. Přináší metody ke snížení rizikové míry plynoucí z přerušení procesů a zavádí mechanismy obnovy. K úspěšné implementaci efektivní ITSCM je nutná plná podpora vrcholového managementu.

Hlavní cíle řízení kontinuity

- udržovat plány IT Service Continuity Plans (ITSCP) a IT Recovery Plans (ITRP), jenž podporují záměry BCP společnosti
- provádět pravidelné revize Business Impact Analysis (BIA) a ověřovat, zda jsou všechny ITSCP v souladu se změnami obchodních dopadů a požadavků
- ověřovat dohodnutou úroveň IT služeb, provádět pravidelné hodnocení rizik Risk assessment (RA), zejména ve spojení s procesy Availability Management a Security Management
- poskytovat rady a návody všem oblastem podnikání, které souvisí s procesy kontinuity a zotavení
- zajistit, že zavedené mechanismy kontinuity a obnovy dosahují odpovídající nebo vyšší úrovně než stanovené cíle
- posoudit dopad všech změn na ITSCP a ITRP
- ujistit se, že proaktivní změny vylepšení dostupnosti služeb jsou implementovány všude tam, kde jsou odůvodněné
- vyjednat smlouvy s dodavateli o poskytování nezbytné podpory pro zajištění obnovy všech plánu kontinuity v návaznosti na proces Supplier Management

ITSCM neřeší drobné technické výpadky, poruchy menšího rázu a očekávaná rizika, jako je porucha nekritického disku či aplikace. K zvládání méně významných problémů z pohledu kontinuity podnikání jsou primárně určeny procesy sdružené v segmentu Service Operation a dále procesy Availability Management, Change Management a Configuration Management.

ITSCM se shodně s koncepcí ITIL nevymezuje na určitý typ společnosti, ale poskytuje doporučení všem poskytovatelům IT služeb. Metody ITSCM lze aplikovat v malém IT oddělení, jenž dodávají IT služby pouze mateřské organizaci, stejně jako ve společnostech, které poskytují své služby jiným organizacím.



Obrázek 1: Životní cyklus řízení kontinuity služeb [4]

2.3 Životní cyklus řízení kontinuity služeb

Životní cyklus řízení kontinuity služeb jak vidíme na obrázku č.1 rozlišuje čtyři základní fáze :

1. Iniciace (Initiation)
2. Požadavky a strategie (Requirements and strategy)
3. Implementace (Implementation)
4. Operace údržby (On going Operation)

2.3.1 Iniciace

První fáze je významná pro organizaci jako celek. Nejprve je nutné zvolit politické nastavení (stanovit manažerský záměr a cíle), definovat pozice, pravomoci a povinnosti zaměstnanců. Určit kdo bude provádět BIA, RA, kontrolní činnosti, kdo zajistí pojištění společnosti a dohled nad dodržování norem. Dále je potřeba alokovat zdroje k vykonání druhé fáze cyklu ITSCM, tedy finance a pracovní síly, ať už z vlastních řad či externích zdrojů, definovat odpovědnost za schvalování projektu, úrovně kvality plánů a zvolit komunikační mechanismy mezi jednotlivými účastníky procesu.

2.3.2 Požadavky a strategie

Tato fáze se zaměřuje primárně na obchodní požadavky, korektní analýzu dopadu - Business Impact Analysis v souvislosti se službami IT, analýzu rizik - Risk Assessment a stanovení efektivní strategie. Strategie dokumentuje požadované opatření ke snížení rizika a možnosti obnovy kontinuity podnikání.

Analýza dopadů (Business Impact Analysis, BIA)

Analýza dopadů identifikuje kritické služby v organizaci a posuzuje finanční ztráty, které vzniknou společnosti např. ztrátou nebo přerušením dodávky služby s ohledem na délku trvání přerušení, ztrátou nebo únikem dat, výpadkem elektrické energie atd.

Kritéria analýzy dopadu

- forma poškození nebo ztráty (ztráta příjmu, dodatečné náklady, poškození reputace, ztráta konkurenční výhody, porušení práva, zdraví a bezpečnosti, riziko pro bezpečnost personálu, okamžitá a dlouhodobá ztráta podílu na trhu, politický, korporační nebo osobní dopad, ztráta způsobilosti)
- rozsah škody nebo ztráta po servisním přerušení v závislosti na délce přerušení (hodiny, dny, měsíce a stanovení nejkritičtější časové hranice)
- počet zaměstnanců, schopnosti, vybavení a služby nezbytné k obnově kritických procesů na minimální přijatelnou úroveň
- minimální čas nutný k dosažení potřebných zdrojů pro zahájení obnovy
- čas, za který je dostupný potřebný personál, zařízení a všechny požadované procesy a služby jsou plně obnovené
- stanovení priority obnovy pro každou IT službu

Hodnocení rizik (Risk Assessment, RA)

Analýza rizik zohledňuje reálnou pravděpodobnost výskytu havárie nebo servisního přerušení, odhaduje úroveň zranitelnosti a rozsah dopadu. Při vyhodnocení analýzy se stanoví míra přijetí, omezení nebo nutnosti úplné eliminace rizika s ohledem na množství vynaložení nezbytných ekonomicky odůvodněných prostředků. Provádí se pro každou IT službu zvlášť. Příklady hrozeb, které zvyšují rizika aktiv ukazuje tabulka č.1 a č.2.

Rizika	Hrozby
Ztráta interních IT systémů nebo sítí	Požár Výpadek napájení Žhářství, vandalismus Povodeň Pád letadla Přírodní katastrofa, např. hurikán Ekologická havárie Teroristický útok Sabotáž Katastrofální selhání Elektrické poškození, např. blesk Náhodnému poškození Nekvalitní software

Tabulka 1: Rizika a hrozby

Rizika	Hrozby
Ztráta externích IT systémů nebo sítí	Všechny výše uvedené Nadměrná poptávka po službách Znepřístupnění služby DoS útokem Selhání technologie
Ztráta dat	Selhání technologie Lidská chyba Viry, škodlivý software
Ztráta síťových služeb	Poškození nebo odepření přístupu k síti poskytovatele služeb Ztráta služeb poskytovatele IT systémů a sítí Ztráta dat poskytovatele služeb Selhání poskytovatele služeb
Nedostupnost klíčového technického a pomocného personálu	Protestní akce Odepření přístupu do prostor Rezignace Nemoc / zranění Dopravní problémy
Výpadek služeb, např. outsourcing IT	Komerční selhání, např. platební neschopnost Odepření přístupu do prostor Nedostupnost zaměstnanců poskytovatele služeb Nesplnění smluvní úrovně služeb

Tabulka 2: Rizika a hrozby - pokračování

Strategie

Výstupy BIA a RA slouží jako základ pro vytvoření strategie s optimální rovnováhou míry rizika a možností obnovy. Strategie musí být integrovatelná do kompletní strategie obnovy kontinuity podnikání společnosti. Priorita obnovení služeb je závislá na délce výpadku služeb a s postupující dobou trvání se mění. Snížení míry rizika služeb s vysokým dopadem z krátkodobého hlediska v rámci BIA se provádí v procesech Availability Managementu, zatímco služby s vysokými dlouhodobými dopady se zahrnují do procesů řízení kontinuity podnikání a plánů obnovy - Disaster Recovery.

Snížení rizik v procesech Availability Managementu

- instalace UPS a záložních zdrojů napájení
- implementace systémů odolných proti poruchám pro kritické aplikace
- RAID pole a duplikace dat na 2 HD pro LAN servery
- náhradní vybavení a součásti pro případ poruchy
- vytvoření nouzového přístupového bodu k síti nebo možnosti napájení budovy
- pružné IT systémy a sítě
- outsourcing služeb zajištěný několika dodavateli
- větší fyzické a IT-BASED bezpečnostní ovládací prvky
- mechanismy pro včasnou detekci hrozby přerušení služby
- komplexní strategie zálohování a obnovy, včetně úložišť v odlehlých lokalitách

Techniky v rámci Disaster Recovery

- Manual work-arounds - krátkodobá náhrada služby manuálním zápisem
- Reciprocal arrangements - dočasné využití služeb a zdrojů jiné organizace
- Gradual recovery 'cold standby' - převedení do záložní lokality připravené k instalaci vlastní výpočetní techniky
- Intermediate recovery 'warm standby' - převedení do plně vybavené komerční lokality, včetně definovaného zařízení (servery, periferie)
- Fast recovery 'hot standby' - převedení do záložní lokality s nainstalovanými IT systémy a aplikacemi, kde jsou zrcadlena provozní data
- Immediate recovery 'mirroring', 'load balancing' ,'split site' - automatické převedení služeb, které jsou implementované ve dvou dostatečně vzdálených rovnocenných lokalitách, uvnitř jedné organizace

2.3.3 Implementace

Ve fázi implementace se sestavují plány ITSCM, které zahrnují potřebné informace k rychlé obnově kritických systémů, služeb a technického vybavení. Dokumentace ITSCM musí být dostupná všem klíčovým zaměstnancům. Distribuci plánu a uložení kopie mimo lokalitu společnosti zajišťuje Management distribuce plánů. Na vývoji a údržbě ITSCM plánů spolupracují týmy specialistů, jejichž činnosti jsou koordinované Business Continuity Managementem (BCM).

Příklad ITSCM plánu obnovy dle doporučení ITIL je zachycen v příloze A.

Kromě stěžejního plánu obnovy je vhodné připojit také některé další záchranné plány a kontaktní informace.

Záchranné plány

- Emergency Response Plan - plán pro nouzové situace
- Damage Assessment Plan - plán odhadu škod
- Salvage Plan - plán likvidačních prací
- Vital Records Plan - plán umístění existenčně důležitých záznamů
- Crisis Management - plán krizového řízení
- Public Relations Plan - plán komunikace s médií
- Accommodation and Services Plan - plán ubytování a služeb
- Security Plan - plán bezpečnosti
- Personnel Plan - personální plán
- Communication Plan - komunikační plán
- Finance and Administration Plan - finanční a administrační plány

Součásti implementační fáze je vytvoření plánu organizace krizového řízení a plánu testování strategie.

Krizové řízení
Úspěšné řízení krizové situace zajišťují tři hlavní organizační jednotky :

- Výkonná – nejvyšší autorita zodpovědná za krizový management
- Koordinační – útvar zodpovědný za koordinaci procesu obnovy
- Jednotka obnovy – obchodní a servisní týmy odpovědné za obnovu služeb

Testování
Účelem testování strategie je prověření sestavených plánů obnovy a odhalení případných nedostatků. Testy musí mít jasně určené cíle a kritické faktory úspěšnosti. Průběh testů se zaznamenává, vyhodnocuje a v případě nutnosti je iniciováno změnové řízení.

Typy testů:

- Walk-through tests - testy pozorováním „za běhu“ týmem tvůrců plánů obnovy
- Full tests – test schopnosti obnovy na určených systémech v požadovaném čase
- Partial tests - doplňkové testy vybraných služeb nebo technického vybavení
- Scenario tests - pro ověření reakcí na specifické podmínky a nečekanou událost

2.3.4 Operace údržby

Pokračující operace nebo-li operace údržby se zaměřují na oblast vzdělávání, zvyšování povědomí, provádění školení, vykonávání pravidelných revizí a ověřování zda plány stále odpovídají potřebám společnosti. Testování plánu kontinuity podnikání se provádí pravidelně, ve shodě s obchodními požadavky a také po každé významné změně. Nutností je prověřování zálohovacích mechanismů a dat potřebných při zotavení služeb IT, což spadá do rámce Service Operation. Veškeré změny obchodních procesů probíhaji řízeně v rámci procesů Change Managementu a Configuration Managementu.

Vyvolání (Invocation)

Invocation je poslední test zajištění obnovy kontinuity podnikání podle sestavených plánů. Pokud všechny předchozí fáze byli úspěšně dokončeny, plány vytvořeny a otestovány, měla by invokace proběhnout bezchybně.

Plány a jejich kopie se uloží na bezpečná místa tak, aby v případě havárie byly k dispozici klíčovému personálu.

Proces zotavení po havárii vede k rychlému zprovoznění kritických IT služeb a jejich poskytování z míst obnovy na úrovni dohodnuté v rámci strategie. Dalším úkolem je pak v nejkratším možném čase převést služby zpět do standardního prostředí společnosti a uvolnit místo obnovy pro případ další havárie. Tyto následné aktivity by měli být rovněž zahrnuty v plánech ITSCM a probíhat řízeně.

3 Zotavení poštovní služby MS Exchange

Poštovní služba MS Exchange se řadí k IT službám, jejichž selhání může mít pro řadu společností vážný dopad na kontinuitu podnikání. Za účelem snížení plánovaných a očekávaných výpadků se implementují poštovní systémy s vysokou dostupností, pokud dojde k neočekávanému selhání dodávky služeb je nezbytné mít k dispozici scénář obnovy.

Riziko, resp. nebezpečí vzniku události, která způsobí narušení systému, ztrátu nebo poškození dat či přerušení dodávky služeb, představují pro každou společnost jiné hrozby. Vedení záznamů neplánovaných výpadků a jejich příčin je pro společnost výhodou a mělo by být součástí identifikace a analýzy rizik.

Průzkum vedený společností MessageOne (poskytovatel emailových systémů) ukazuje, že téměř 86% neplánovaných výpadků je způsobeno technologickým selháním a jen 14% zapříčiňují přírodní katastrofy. Nejčastější příčiny neplánovaných výpadků a jejich procentuální zastoupení je znázorněno na obrázku č.2.

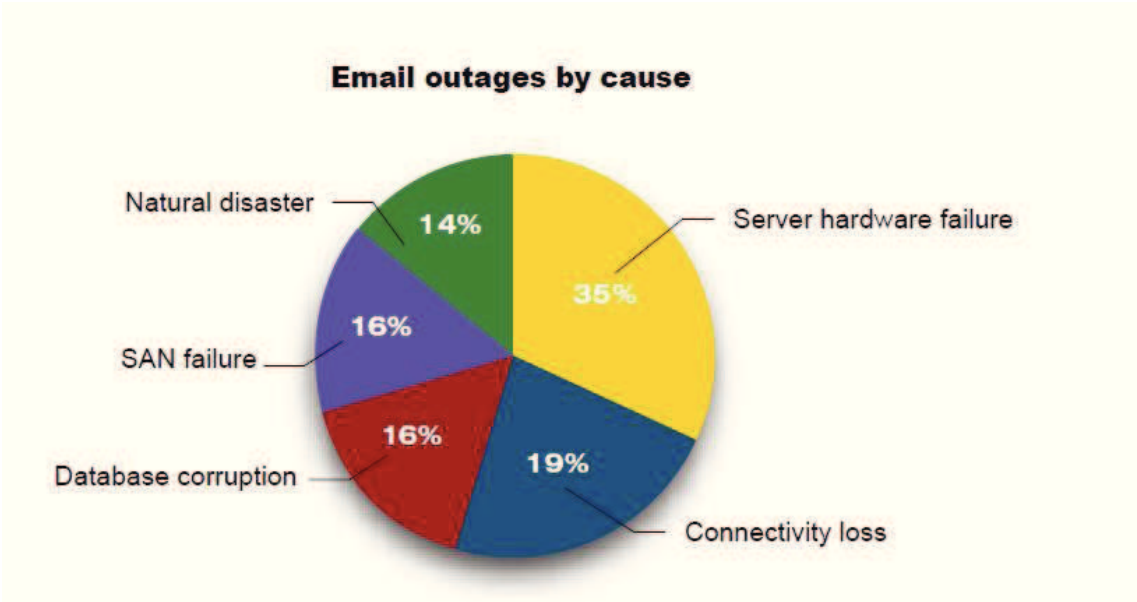
Z výsledků je patrné, že vhodně navrženou infrastrukturou IT, která respektuje zásady systémů vysoké dostupnosti lze eliminovat také významnou část vzniku neplánovaných výpadků. Kompletní zpráva průzkumu se nachází na webových stránkách www.disaster-resource.com.
http://www.disaster-resource.com/articles/ems_whitepaper_why_emls_fail.pdf

3.1 Rizika poštovních služeb

Riziko v bezprostřední souvislosti s poskytováním poštovních služeb vzniká zejména ztrátou či poškozením následujících instancí:

- položka z mailboxu (email, složka, obsah kalendáře, úkoly atd.)
- celý mailbox
- databáze nebo skupina úložišť
- poštovní server nebo role
- externí služby (Domain Controller, Global Catalog, DNS, LAN, WAN)
- ztráta celé lokality (Exchange server a veškeré externí služby)

Pro efektivní sestavení plánů obnovy je potřeba znát, která data jsou důležitá, kde se nachází a jak je správně zabezpečit. Architektura poštovního systému Exchange server společnosti Microsoft doznala ve verzi 2007 významných změn. Poštovní systém je koncipován jako systém serverových rolí, jenž mohou být instalovány na jeden nebo více fyzických popř. virtuálních hostitelů dle individuálních potřeb společnosti. Možnost instalace redundantních serverových rolí, korektní konfigurace systému a pravidelné zálohování přispívá ke zvyšování odolnosti Exchange serveru.



Obrázek 2: Příčiny neplánovaných výpadků [7]

Konfigurace MS Exchange Serveru je z větší části uložena v adresářové službě Active Directory. Zotavení poštovního serveru nebo jeho role se vykoná spuštěním instalace v režimu obnovy po havárii a všechna základní nastavení jsou obnovena z AD (za předpokladu, že je adresářová služba k dispozici), příp. doplníme o uživatelské nastavení ze záloh. Při havárii mailbox serveru rovněž obnovíme poškozené databáze.

3.2 Kritická data MS Exchange serveru

Mailbox server

- Mailbox databáze a databáze veřejných složek
- Transakční logy pro každou skupinu úložišť
- Windows registry

K záloze databáze a transakčních logů se zpravidla využívá zálohovací mechanismy třetích stran s podporou zálohování Exchange serveru nebo backup služba implementovaná v serverových operačních systémech společnosti Microsoft. Windows registry uchováme v rámci zálohy System state nebo je vyexportujeme. Ve verzi Microsoft Exchange server 2010 je implementována nová technologie Database Availability Group (DAG) s tzv. lagged copy, což znamená, že existuje tzv. jedna živá databáze a k ní několik jiných kopií na různých serverech, z nichž jedna má zpožděný (lagged) zápis transakčních logů, řádově i několik dní.

Hub transport server
- Fronty zpráv
- Logy pro sledování zpráv
- Windows registry

Fronty zpráv se nezálohují, ale pokud při poškození serveru se tyto fronty podaří obnovit, mohou být přeneseny na nový server. Logy pro sledování zpráv lze zálohovat na úrovní souborového systému. Windows registry vyexportujeme nebo zálohujeme pomocí System state. Záloha transakčních logů a registrů není k obnově funkce HUB serveru nezbytná.

Edge transport server
- konfigurace ADAM - Active Directory Application Mode
- konfigurace ESE - Extensible Storage Engine

Záloha je nutná pouze pokud jsme provedli vlastní nastavení. Pro usnadnění zálohy je v instalační sadě MS Exchange serveru připraven script ExportEdgeConfig.ps1 a také ImportEdgeConfig.ps1 pro obnovu konfigurace. Výchozí nastavení není potřeba zálohovat.

Client Access Server
- Outlook Web Access
- Nastavení IMAP4 a POP3
- Availability service
- Exchange ActiveSync
- Outlook Web Access virtual directories
- Autodiscover
- konfigurace Web services (IIS)
- Windows Registry

Největší počet služeb poštovního serveru a tedy i konfiguračních souborů se nachází na CAS serveru. K zabezpečení potřebných dat se obvykle využívá záloha na úrovni souborů a záloha System state.

Unified Messaging (UM)
- vlastní soubory (.wav)

Pokud poštovní server využívá hlasové služby s vlastními audio soubory, provádíme zálohy těchto souborů, v opačném případě záloha není nezbytná.

3.3 Obnova poštovních služeb

V této chvíli je zřejmé, která data poštovního serveru je potřeba zálohovat. Nyní přiblížím obnovu dříve uvedených rizikových instancí. Nejprve připomenu snadnější varianty obnovy při poškození nebo ztrátě položek, mailboxu a databáze nebo skupiny úložišť, kdy

poštovní server nebyl zasažen a je plně funkční. Poté přistoupíme k obnovám při ztrátě poštovního serveru, externích služeb a celé lokality.

Obnova položky mailboxu

Prvním stupněm ochrany před ztrátou položky z mailboxu je nastavení vhodné retenční politiky. Retence je ochranná doba od okamžiku ztráty, kdy smazané položky mailboxu mohou být obnoveny pomocí klienta Outlook nebo Outlook web access (OWA). Výchozí délka retence je 14 dní.

Pokud nelze využít obnova obsahu mailboxu v retenční lhůtě, přistoupíme k obnově ze zálohy. Způsob obnovy je popsán v části obnova databáze nebo skupiny úložišť, jelikož bez zálohy databáze je obnova mailboxu a tedy jeho obsahu nemožná.

Obnova celého mailboxu

Podobně jako v předchozím případě je mailbox chráněn určitý časový úsek před úplným smazáním. Při smazání je mailbox nejprve označen k odstranění. S tímto značením je chráněn retenční politikou, tzn. je uchován jako odpojený a lze jej snadno obnovit připojením k AD účtu. Po uplynutí ochranné doby se teprve mailbox, pokud nebyl obnoven, stane kandidátem na tvrdé smazání a při řádné automatické údržbě databáze je definitivně smazán. Výchozí nastavení retence pro mailbox je 30 dní.

Retenční politika pro obsah mailboxu i celý mailbox se nastavuje na Exchange serveru. Zvyšování délky ochranného období se provádí uváženě s ohledem na velikost databáze, kapacitu disku a délku zálohování.

Mailbox, který byl definitivně smazán, se nově vytvoří a jeho obsah se obnoví ze zálohy databáze jak ukáže následující část.

Obnova databáze nebo skupiny úložišť

Obnovu ze zálohy je možné využít při ztrátě položky mailboxu, celého mailboxu a také při ztrátě databáze nebo skupiny úložišť. Jak dlouhou dobu lze k obnově uvedených dat využít zálohu závisí na vlastním nastavení zálohovacích systémů. Zálohování plánujeme zpravidla periodicky v denních, týdenních či měsíčních intervalech.

Recovery Storage group (RSG)
Obnova obsahu mailboxu a celého mailboxu se provádí na úrovni obnovy skupiny úložišť. Konkrétní kroky obnovy jsou závislé na užívaném zálohovacím systému, avšak vždy postupujeme od největšího zálohovaného celku - skupiny úložišť, kterou obnovíme do zvolené administrační lokace RSG. Jedná se o speciální úložiště pro připojení databáze poštovních schránek, které nejsou běžným uživatelům dostupné.

Obsah vybraných mailboxů lze překopírovat do složky v aktivní poštovní schránce nebo přímo sloučit se stávajícím mailboxem. Obnova položek se vykonává shodně s obnovou

mailboxu, kdy finální lokalizace požadovaných dat, příp. utřídění obsahu mailboxu, je na uživateli.

Výběrem všech mailboxů a jejich sloučením s jednotlivými poštovními schránkami lze provést obnovu celé databáze. Pokud není obnova do stávajících poštovních schránek vhodná, máme k dispozici plný přepis stávající databáze obnovenou databázi ze zálohy. Takto obnovíme stav poštovních schránek k určitému datu a změny po tomto datu nemusí být zachovány.

Přepis stávající databáze
Pokud došlo k poškození celé databáze, tzn. nebudeme obnovovat jen určitá data ze zálohované databáze, můžeme přistoupit k obnově přímým přepisem přes stávající poškozenou databázi. V tomo případě se nevyužívá RSG, ale obnova je směrována do původního umístění databáze a transakčních logů.

Dial-tone
Další možnost obnovy databáze je tzv. obnova „dial-tone“. Proces obnovy probíhá v několika krocích. Nejprve je obnovena databáze s prázdnými, avšak funkčními mailboxy. Dále se standardním způsobem do RSG realizuje obnova databáze ze zálohy, provede se výměna obou databází a na závěr se sloučí nová data z původním obsahem mailboxů.

Obnova „dial-tone“ přináší velmi rychlý způsob zprovoznění funkčnosti mailboxů pro příjem i odesílání e-mailové komunikace. To může být přínosné z pohledu kontinuity podnikání, zejména pokud k vyřizování elektronické komunikace není původní obsah mailboxů v aktuálním čase nezbytný, příp. je-li v rámci firemní politiky prováděna archivace kritických dat na straně klienta a lze přechodnou dobu překrýt použitím klienta Outlook s mezipamětí (Cached exchange mode) nebo využitím ukládaných dat do osobních složek (Personal folders).

Obnova zálohy z pásky
Potřebujeme-li obnovit mailbox nebo databázi ke staršímu datu než nám poskytuje záloha nebo jsou-li zálohovaná data poškozená, je potřeba nejprve získat data z archivních médií. Z archivních dat se vyselektují soubory databází a transakčních logů, které se nakopírují do zvoleného místa obnovy. Délka ochrany dat je opět závislá na potřebách společnosti, nastavení archivačního zařízení a životnosti archivačních médií .

Obnova fyzického serveru

Instalace nového fyzického serveru
Selhání nebo poškození poštovního serveru mnohdy vyžaduje zprovoznění nového fyzického stroje. Zotavení se provede obnovou stavu systému na podobném hardwaru nebo čistou instalací. Hardwarovými parametry serveru, instalaci odpovídajícího OS a potřebnými komponenty pro běh Exchange Serveru se nebudeme zabývat, jelikož toto

není náplní práce. V rámci DR by veškeré potřebné údaje včetně technických požadavků měly být pečlivě zdokumentovány.

Mějme tedy nainstalovaný server, opatřený OS a připravený k obnově poštovního serveru. Server musí nést jméno shodné s poškozeným serverem, musí být zařazen v příslušné AD doméně a mít obnoven účet počítače.

Zotavení Exchange Serveru se provede instalací s přepínačem pro obnovu systému , kdy se na server aplikuje základní nastavení z AD. V dalším kroku se obnoví potřebná konfigurační nastavení podle instalované role poštovního serveru (viz. kapitola 3.2).

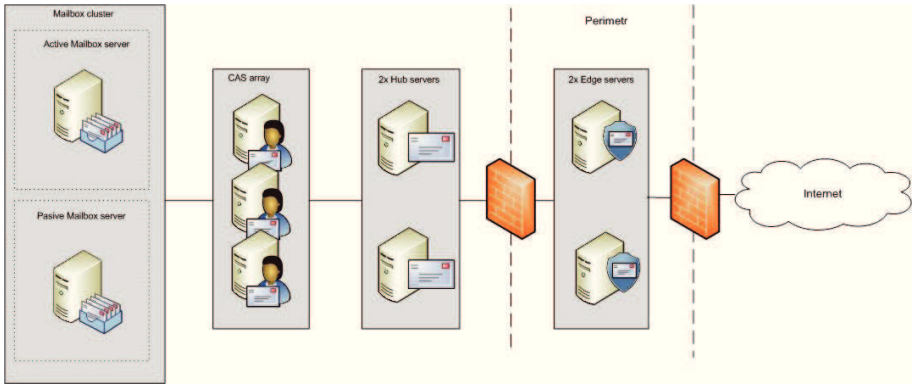
Je-li předmětem zotavení role Mailbox je nutné obnovit všechny skupiny úložišť poštovních schránek nebo databáze veřejných složek. Pokud jsou databáze větší velikosti může být výhodou provádění záloh metodou stínové kopie svazků – Volume Shadow Copy (VSS), kdy proces obnovy významně zkrátí čas nutný k zprovoznění databází.

Doinstalace role na jiný server
Poštovní systém, jehož role jsou implementované na samostatných servrech, můžeme za určitých okolností obnovit přidáním, resp.doinstalací poškozené role na další server. Na jednom fyzickém serveru mohou být nainstalovány všechny základní role Exchange serveru - Mailbox, HUB, CAS. Kombinace těchto rolí, pokud nevyužívají řešení clusteru, není z pohledu funkčnosti poštovního serveru omezena. Restrikce vyplývají pouze z potřeb společnosti, infrastruktury Exchange serveru a implementovaného HW.

Převzetí služeb jiným členem clusteru
Exchange server, resp. role seskupené do clusteru se implementují ve společnostech, kde je nutná vysoká míra zabezpečení a odolnosti proti výpadkům služby. Každá z rolí poštovního serveru může být instalována na jednom či více poštovních serverech v každé AD site s implementovaným Exchange serverem. Redundance serverových rolí Hub, CAS, Edge a UM pozitivně ovlivňuje rozložení zátěže a zvyšuje tak dostupnost služeb, zatímco hostováním mailbox serveru na clusteru se snižuje riziko poškození a ztráty databází, příp. lze poškozenou databázi rychle obnovit. Příklad zapojení Exchange serveru s využitím clusteru u jednotlivých serverových rolí je znázorněno na obrázku č.3.

Technologie vyrovnání zátěže
- Hardwarový load balancer – hw zařízení pro rozklad zátěže na síťové vrstvě
- Network load balancer (NLB) – softwarové řešení integrováno v serverových OS
- DNS round robin

Vícenásobná instalace role Hub transport serveru nevyžaduje žádné zvláštní zařízení ani hostování na clusteru. Vysoká dostupnost a řízení přepínání probíhá mezi všemi Hub Transport servery automaticky.



Obrázek 3: Exchange server – infrastruktura s využitím clusteru

Rozložení zátěže přístupových CAS serverů se dosahuje implementací NLB nebo začleněním hardwarového load balanceru do síťové infrastruktury. Microsoft Exchange server 2010 pak přináší technologii CAS array, která vyvažuje zátěž vyvolanou požadavky klientů na přístup k mailboxům a tím redukuje možnost výpadku. V každé AD site může být pouze jeden CAS array a všechny CAS servery jsou jeho členy. CAS array umí využívat jak hardwarový tak softwarový load balancer.

Redundance Edge Transport serveru může obdobně jako CAS server využívat load balancer na softwarové úrovni – NLB nebo navozovat vyrovnání zátěže přidáním více MX záznamů do DNS.

Rozložení zátěže hlasových služeb při nasazení redundantní role Unified Messaging zajišťuje služba DNS round robin.

Role Mailbox lze konfigurovat pro použití clusteru typu Local Continuous Replications (LCR), Standby Continuous Replications (SCR) a Cluster Continuous Replications (CCR). Výběr typu clusteru je podmíněn verzi Exchange serveru. Implementace tzv. geoclusteru na bázii CCR je velmi silným technologickým řešením z pohledu prevence i řízení rizik širokého spektra dopadů možných havárií a přírodních katastrof.

Použití technologie clusteru s sebou přináší další eventuality výpadků a nutná řešení. Scénáře obnovy pak zachycují rozdílné postupy při selhání jednoho člena v clusteru, kdy je funkce dočasně nahrazená jiným členem, a při havárii celého clusteru, kdy je určitá role zcela nedostupná a omezuje nebo zcela přerušuje dodávku poštovních služeb.

Obnova lokality

Při ztrátě celé lokality probíhá obnova ve dvou scénářích :
1. obnova bez záložní lokality
2. obnova v záložní lokalitě

Obnova bez záložní lokality

Vybudovat a udržovat záložní lokalitu je pro mnohé společnosti vzhledem k výraznému finančnímu zatížení neakceptovatelné. Proces obnovy služeb ve stávající lokalitě pak závisí nejen na zálohách dat, které máme k dispozici, ale také na dopadu katastrofy na podnikání jako celek. Zotavení poštovních služeb je součástí řízené obnovy kontinuity podnikání a závisí na mnoha faktorech. Po provedení odhadu škod se rozhodne jestli investice do zotavení podnikání je přijatelná, jestli je lokalita obnovy schopná (zemětřesení) a zda spustit proces obnovy je dostatečně bezpečné (další otřesy) atd.

Zahájení obnovy poštovních služeb, ať už ve stávající či nové lokalitě, přichází na řadu ve chvíli, kdy je vybudována, resp.obnovena infrastruktura IT (počítačová síť s adresářovou službou AD). Samotné zotavení poštovního serveru probíhá způsobem popsaným v části obnova poštovního serveru nebo role.

Obnova v záložní lokalitě

Záložní lokalita je zpravidla geograficky odlehlá oblast vybavená IT infrastrukturou. Její význam a účel vybudování se různí s ohledem na potřeby a možná rizika společnosti. Záložní lokalita může sloužit jako pouze bezpečné úložiště zálohovaných dat, jako záložní řešení pro převzetí služeb při výpadku produkční lokality, nebo jako plnohodnotná lokalita s plně automatizovaným systémem převodu služeb (failover). Způsob a čas potřebný k obnově poštovních služeb pak závisí na zvoleném typu záložní lokality.

Microsoft Office 365 – hostování v Microsoft cloud

S příchodem Microsoft Exchange Serveru 2010 se objevila možnost úplného nebo částečného hostování poštovních služeb v cloudu. Cloudové řešení lze využít jako kompletní řešení poštovních služeb na bázi Exchange, ale také jako specifický typ záložní lokality.

Samotná technologie cloudu zaručuje uživateli nepřetržitý přístup k mailboxu z libovolného místa připojení. Zajištění nepřetržité dodávky služeb je součástí návrhu sady Office 365. Tato ustanovení umožňují rychlé zotavení služeb Office 365 z neočekávaných událostí jako jsou selhání hardwaru nebo aplikace, poškození dat a dalších událostí, které mají vliv na uživatele. Řešení kontinuity služeb se uplatňují rovněž v případě katastrofických výpadků jako jsou přírodní katastrofy nebo požár v datacentru společnosti Microsoft, které mohou způsobit nefunkčnost celého centra.

Dostupnost služeb a zákaznických dat v cloudu Office 365 je zajištěna technikami ukládání a zálohování dat, monitorováním a údržbou systému.

Ukládání dat a zálohování

Pro zajištění dostupnosti, kontinuity podnikání a rychlého zotavení po havárii jsou data zákazníků uložena v redundantním prostředí s robustním zálohováním, obnovou a schopností automatického převzetí služeb. Redundance dat je zajištěna na více úrovních, od redundantních disků na ochranu před selháním lokálních disků až po úplnou replikaci

dat do geograficky odlišných datových center.

Monitorování a údržba
Hlavním účelem monitorování a údržby je předcházet možnému snížení výkonnosti nebo celkovému selhání systému a zabránit ztrátě dat. Databáze jsou pravidelně kontrolovány na na blokované procesy, ztrátu paketů, fronty procesů a skryté (latentní) dotazy.

Preventivní údržba zahrnuje pravidelné kontroly konzistence databází, periodické provádění kompresí dat a sledování protokolu chyb.

Obnova externích služeb

Poštovní server MS Exchange se integruje do interní struktury AD společnosti. Adresářová služba slouží k uložení konfigurace poštovního serveru, dále se využívá k ověřování uživatelů a vyhledávání informací o objektech exchange organizace. Z pohledu externích služeb je tedy pro běh Exchange serveru nezbytná funkčnost Domain Controlleru (DC) a Global Catalogu (GC).

Datové přenosy mezi účastníky elektronické komunikace (poštovní servery, odesilatelé a příjemci) zajišťují síťové prostředky a služby DNS, LAN až po připojení k WAN síti. Výpadky ve WAN síti jsou z pohledu obnovy mimo kompetence společnosti, avšak v případě potíží je nutné znát kontaktní místo poskytovatele, kde lze poruchu ohlásit.

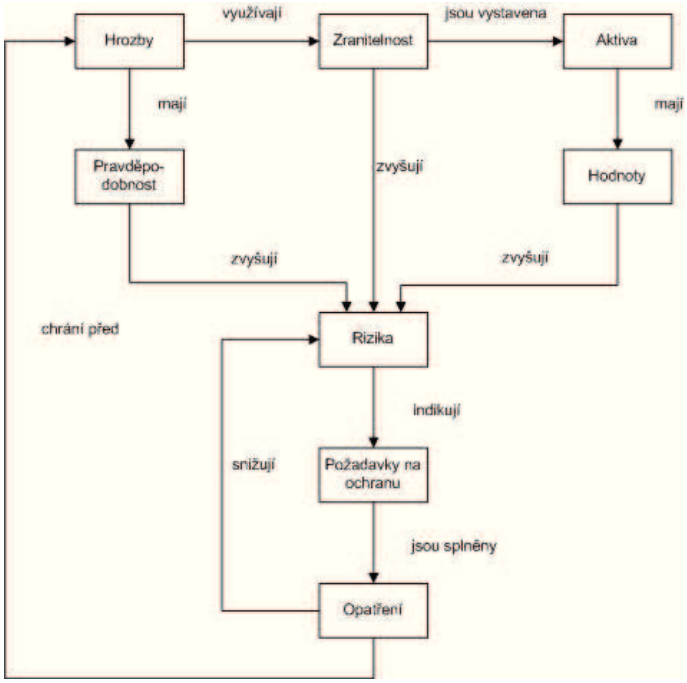
K externím službám v závislosti na firemní infrastruktuře zahrnujeme také další služby a aplikace např. spam filtry, zálohovací a archivační zařízení, jejichž poruchou nebo nedostatečnou funkčností nedojde k okamžitému selhání poštovního systému. Ovšem dlouhodobá disfunkce těchto služeb by mohla mít fatální dopad na kontinuitu podnikání v budoucnu.

Obnova externích služeb se zpravidla řeší samostatně, přesto je potřeba být si jednotlivých závislostí vědomi a v rámci plánů disaster recovery vést odkazy na příslušné dokumenty a odpovědné osoby.

3.4 Plán zotavení po havárii

Plán zotavení poštovní služby MS Exchange je založen na doporučení ITIL a čtyřech fázích životního cyklu řízení kontinuity služeb:

1. iniciace
2. analýza rizik
3. implementace
4. operace údržby



Obrázek 4: Analýza rizik

Iniciace

Iniciační fáze je nezbytnou součástí každého plánu. Stanoví se hlavní cíl, rozsah zabezpečení poštovních služeb, definuji se kompetence a případné další podmínky či omezení dle potřeb společnosti.

Analýza rizik

V této fázi se identifikují a ohodnotí aktiva, tj. hardware, software, služby a další zdroje, které mají z pohledu zajištění kontinuity poštovních služeb hodnotu a musí být odpovídajícím způsobem chráněné.

Dále se identifikují hrozby - události, které mohou mít negativní dopad na dodávku poštovních služeb a stanoví se, s jakou pravděpodobností může hrozba ve společnosti způsobit havárii.

Nezbytným hlediskem analýzy rizik je určení zranitelnosti aktiv. Zranitelnost udává míru poškození aktiva určitým typem hrozby.

Výsledné riziko poštovního systému se vypočítá z hodnot aktiv, míry zranitelnosti a pravděpodobnosti, že hrozba využije zranitelnosti aktiva. Hodnocení rizik je tedy specifická záležitost pro každou společnost a odpovídá určeným hodnotám aktiv, zranitelnosti a pravděpodobnosti.

Závěrem se dvojice aktiv a hrozeb seskupí do kategorií dle úrovně rizika. Navrhnou se vhodná preventivní opatření, monitorovací systémy a způsoby zabezpečení za účelem částečné nebo úplné eliminace rizik. Tam, kde riziko dosahuje kritické úrovně se navíc ve fázi implementace vypracují scénáře obnovy poškozených aktiv.

Proces analýzy rizik je zachycen na obrázku č.4.

Implementace

V implementační fázi se pracuje se seznamem kritických rizik. Vyhotovují se scénáře řízené obnovy a také další nezbytné plány a dokumentace, jenž souvisí s procesy včasné a úspěšné obnovy poštovních služeb nebo její části. Charakter a rozsah dokumentace se volí podle individuálních potřeb společnosti.

Výstupem je pak soubor plánů a dokumentů :

- dokument organizace společnosti
- dokument krizového řízení společnosti
- dokument infrastruktury Exchange serveru a fyzické lokace
- technická dokumentace
- dokument konfigurace Exchange serveru
- dokument externích služeb Exchange serveru
- dokument umístění instalačních medií a datových záloh
- plány údržby systému
- plány zálohování a archivace dat
- plán scénářů řízené obnovy
- scénáře řízené obnovy poštovních služeb
- plán testování scénářů DR
- plán školení zaměstnanců pro účely obnovy systému
- evidence neplánovaných výpadků a havárií

Operace údržby

Pro úspěšné zajištění obnovy je nutné nadále celý proces sledovat, vyhodnocovat a zapracovávat případné změny v požadavcích na sjednanou úroveň služby a infrastrukturu. Revize vytvořených plánů Disaster Recovery, stejně jako testování použitelnosti zálohovaných dat a schopnosti obnovy systému nebo jeho části se provádí opakovaně alespoň jedenkrát ročně. Dále je potřeba seznámit s plány obnovy dostatečné množství personálu a proškolit účastníky samotného procesu obnovy.

4 Analýza rizik v modelové společnosti

4.1 Popis společnosti

Modelem společnosti, pro implementaci plánů Disaster recovery poštovních služeb na bázi Microsoft Exchange, je centrálně řízená firma s 5000 zaměstnanci. Společnost poskytuje své služby v hlavním sídle a deseti pobočkách v převážně evropských zemích. S ohledem na nutnost nepřetržitého provozu je pro společnost kritická vysoká dostupnost služeb a bezpečnost dat elektronického poštovního systému.

Elektronickou komunikaci ve společnosti zprostředkovává Exchange server 2007, který je umístěn ve dvou datových střediscích tak, aby splňoval požadavky na škálovatelný, bezpečný a vysoce dostupný systém (obrázek č.5). Obě datové lokality jsou součástí firemní síťové infrastruktury s AD strukturou a vysokorychlostním připojením k internetu. Správa lokalit je zajištěna centrálním týmem administrátorů.

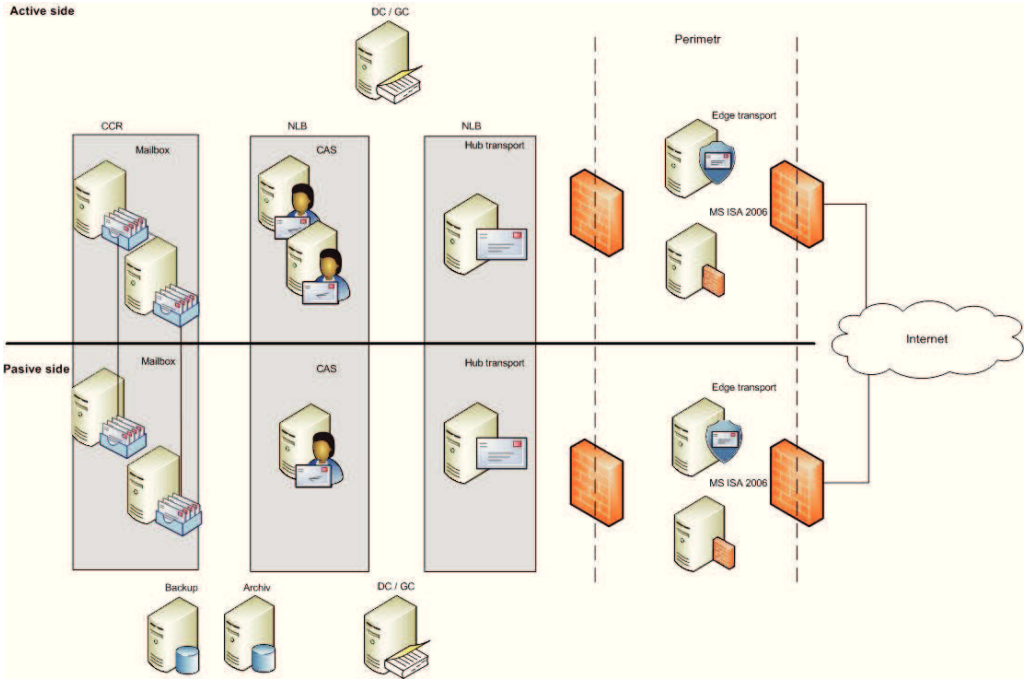
Všichni uživatelé využívají plný přístup ke všem službám Exchange serveru nepřetržitě, tj. 24hodin denně po 7 dní v týdnu. Využívat lze globální seznamy adres, kontakty, sdílené kalendáře, mailboxy a další zdroje. Poštovní schránky jsou pro uživatelé dostupné jak z interní tak z externí sítě. Standardními klienty jsou MS Outlook a webové rozhraní. Pro připojení přes webové rozhraní se využívá zabezpečený přístup. Profily uživatelů MS Outlook jsou konfigurovány pro užití režimu s mezipamětí - Exchange Cached mode, která umožňuje práci offline. K poštovní schránce se lze připojit také pomocí mobilního přístroje.

Infrastruktura

Exchange server 2007 je umístěn ve dvou datových centrech. Lokalita „active site“ je primárně využívaná pro standardní běh poštovních služeb. Oblast „passive site“ je určená jako plnohodnotná záložní lokalita pro zajištění provozu a automatické převzetí služeb při plánovaných výpadcích i neplánovaných haváriích v primární lokalitě.

Mailbox
V aktivní lokalitě jsou umístěny 2 mailbox servery zapojeny v Cluster Continuous Replication (CCR), jejichž data, transakční logy poštovních databází jsou průběžně replikovány do pasivní lokality. Takto jsou mailbox databáze udržovány na záložních serverech a připraveny k okamžitému manuálnímu či plně automatickému převzetí služeb bez ztráty dat.

CAS
Role Client Access Server zprostředkovává přístup k mailboxům všemi klienty vyjma MS Outlook a to včetně připojení z externí sítě přes ISA server. Dále CAS server poskytuje informace o volném čase (FreeBusy), o zprávách Mimo kancelář (Out of Office), podporuje automatické nastavení uživatelského profilu a přístup k Offline adresáři.



Obrázek 5: Infrastruktura modelové společnosti

Pro zajištění vysoké dostupnosti a rozložení zátěže je role CAS nainstalována na dvou serverech aktivní lokality a jednom serveru pasivní lokality. Všechny CAS servery jsou členy Windows NLB clusteru.

Webový přístup je zabezpečen nainstalovaným SSL certifikátem na všech serverech s CAS rolí. Z internetu jsou klienti směrováni nejprve na server ISA umístěný v perimetru sítě společnosti, kde je provedena autentizace uživatele.

Hub Transport
Serverová role Hub Transport, která je určena k směrování elektronické pošty do poštovních schránek mailbox serveru interním příjemcům nebo externím příjemcům do internetu, je nasazena na dvou fyzických serverech. Servery jsou umístěny po jednom v každé z lokalit a jsou, obdobně jako CAS servery, spojeny v NLB clusteru.

Pro zajištění antivirové ochrany je na obou Hub Transport serverech společnosti nainstalován Forefront Security for Exchange Server

Edge Transport
Edge Transport server je umístěn na hranici topologie aktivní i pasivní lokality a plní funkci antispamové ochrany. Spam, nevyžádaná pošta, se podílí téměř 90 procenty na celkovém objemu elektronické komunikace a je žádoucí tuto komunikaci odfiltrovat v

perimetru síťové infrastruktury. Antivirovou ochranu zajišťuje na Edge serverech rovněž Forefront Security.

MX záznamy pro příjem pošty z internetu jsou směrovány na oba nasazené Edge servery. Korektní příchozí externí komunikace je směrována na Hub Transport servery, odchozí komunikace z interní sítě je směrována do internetu.

ISA Server
ISA server zajišťuje ověření identity uživatelů, kteří přistupují ke svým poštovním schránkám klienty z prostředí internetu. ISA server je umístěn taktéž v perimetru topologie obou lokalit. Přístup k mailboxům z Internetu má z pohledu zajištění kontinuity služeb nižší prioritu.

Zálohování a archivace
Zálohovací a archivační zařízení je umístěno v pasivní lokalitě. Zálohování je prováděno systémem Symantec Backup Exec 12.5 (BE) na disková pole a dále jsou zálohy pomocí softwaru Hiback ixT ukládány na pásky. Páskové nosiče jsou umístěny v protipožární místnosti.

4.2 Analýza dopadu

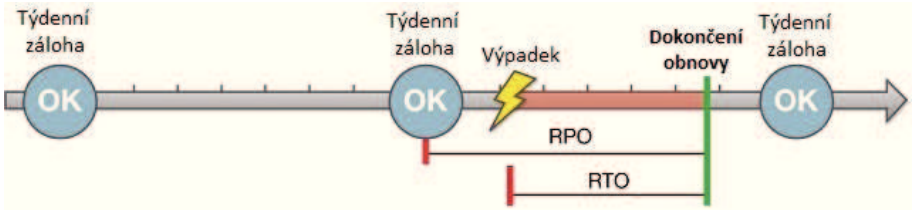
Za analýzu obchodních dopadů a posouzení finančních ztrát, které vzniknou poškozením dat nebo nedostupností elektronického poštovního systému, je odpovědné obchodní oddělení společnosti. Z výsledků této analýzy jsou pro řízenou obnovu systému důležité limity stanovené pro čas potřebný k obnově - Recovery Time Objective (RTO) a tzv. bod v čase, ke kterému se obnova provede - Recovery Point Objective (RPO).

Recovery Time Objective (RTO)
RTO vymezuje nejdelší přijatelný časový limit k provedení obnovy systému nebo jeho částí, které jsou kritické z pohledu kontinuity podnikání. Jedná se o významná obchodní data, mailboxy, poštovní databáze, servery nebo role a externí služby.

Maximální čas obnovy je stanoven na 24h, tzn. že doba obnovy jednotlivých instancí by měla být menší než 24h tak, aby obnova celého poštovního systému a jeho okolí nepřesáhla 24h.

- obnova kritického mailboxu nebo jeho obsahu musí být provedena do 1h
- v případě pádu celého poštovního systému nesmí doba obnovy přesáhnout 24h
- obnova externích služeb a okolí systému se řídí samostatně, avšak celková délka obnovy včetně poštovních služeb nepřesáhne 24h.

Recovery Point Objective (RPO)
RPO definuje maximální vzdálenost bodu obnovy tak, aby ztráta dat byla z pohledu dopadu pro společnost přijatelná. Data musí být dostatečně zabezpečená, aby se v případě obnovy po havárii systém vrátil k bodu havárie, nejdále však o určené RPO.



Obrázek 6: Časová osa obnovy

Čím je tato hodnota nižší, tím je bod obnovy blíže k okamžiku havárie a v ideálním případě je tato hodnota rovná nule. Tj. obnova systému je vykonána bez ztráty dat.

- Bod obnovy RPO nesmí přesáhnout 24h

Časová osa obnovy a souvislost s RTO a RPO je zachycena na obrázku č.6.

4.3 Analýza rizik

Analýzu rizik poštovní služby Exchange server 2007 v modelové společnosti zahájím identifikací aktiv a hrozeb, dále sestavením matice zranitelnosti a vypočtu míru rizika.

Aktiva

Aktiva zahrnují veškeré technické vybavení, software, data, dokumentace, prostory a služby, které jsou potřeba chránit před ztrátou nebo poškozením. Aktiva, resp. jejich význam pro společnost, vyčíslíme podle pětibodové stupnice takto :

1. velmi nízký význam
2. nízký význam
3. střední význam
4. vysoký význam
5. kritický význam

Typ	Název aktiva	Hodnota
hardwarové vybavení	A1 Exchange server	5
	A1.1 Mailbox server	5
	A1.2 CAS	4
	A1.3 Hub Transport	3
	A1.4 Edge Transport	3
	A2 ISA Server	2
	A3 Backup server	3
	A4 Disková pole	5
	A5 Síťové prvky	4

Tabulka 3: Aktiva, ohodnocení

Typ	Název aktiva	Hodnota
software	A6 OS MS Windows 2008	4
	A7 MS Exchange 2007	4
	A8 MS ISA 2007	3
	A9 Backup Exec	4
	A10 Hiback ixT	3
	A11 Forefront Security	2
data	A12 data Exchange serveru	5
	A12.1 položky mailboxu	4
	A12.2 mailboxy uživatelů a sdílené	4
	A12.3 Mailbox databáze	5
	A13 konfigurace	4
	A13.1 konfigurace Mailbox server	4
	A13.2 konfigurace CAS	4
	A13.3 konfigurace Hub Transport	1
	A13.4 konfigurace Edge Transport	2
	A14 zálohy dat	5
služby	A15 CCR cluster (Mailbox)	5
	A16 NLB cluster (CAS,HUB)	5
	A17 Active Directory (DC,GC,DNS)	3
	A18 síťové služby (LAN, WAN)	4
dokumentace	A19 Technická dokumentace	4
	A20 Dokumentace konfigurací a změn	4
	A21 Smlouvy poskytovaných služeb	4
prostory	A22 aktivní lokalita	5
	A23 pasivní lokalita	5

Tabulka 4: Aktiva, ohodnocení - pokračování

Hrozby

Hrozby poštovního systému zahrnují vše, co může způsobit přerušení dodávky služeb, snížení kvality, ztrátu dat nebo celkovou havárii systému. K jednotlivým hrozbám odhadnu míru pravděpodobnosti, že hrozba negativně ovlivní běh poštovních služeb a uvedu příklady zranitelnosti. Ke klasifikaci hrozeb opět použiji 5 stupňů (1. velmi nízká pravděpodobnost - 5. velmi vysoká pravděpodobnost).

Název hrozby	Příklad zranitelnosti	Pravděpodobnost
H1 Selhání SW	nedodržení aktualizace	3
H2 Selhání HW	nedostatečná údržba	4
H3 Selhání sítě, nedostupnost	nedodržení smluv, technické problémy	4
H4 Selhání administrátora	nedostatečné znalosti	4

Tabulka 5: Hrozby, pravděpodobnost

Název hrozby	Příklad zranitelnosti	Pravděpodobnost
H5 Selhání uživatele	nedostatečné znalosti	5
H6 Provozní selhání	nedostatečný servis	3
H7 Výpadek elektrické energie	nedodržení smluv, technické problémy	2
H8 Porucha klimatizace	nedostatečná údržba	2
H9 Vandalismus	úmyslné poškození	4
H10 Krádež	nedostatečné zabezpečení	3
H11 Útoky na síť, aplikaci	úmyslné poškození	5
H12 Požár	možné nebezpečí požáru	2
H13 Blesk	přírodní katastrofa	3
H14 Záplava, zemětřesení	přírodní katastrofy	1

Tabulka 6: Hrozby, pravděpodobnost - pokračování

Zranitelnost

V okamžiku, kdy znám hodnotu aktiv a pravděpodobnost hrozeb, přistoupím k sestavení matice zranitelnosti. Matice vyjadřuje vztah identifikovaných aktiv a hrozeb. Tento vztah opět ohodnotím dle potřeb společnosti a hodnotu vyjádřím číslem 1-5.

1. velmi nízká zranitelnost
2. nízká zranitelnost
3. střední zranitelnost
4. vysoká zranitelnost
5. velmi vysoká zranitelnost

Aktiva	Hrozby	H1 3	H2 4	H3 4	H4 4	H5 5	H6 3	H7 3	H8 3	H9 4	H10 3	H11 5	H12 3	H13 3	H14 1
A1	5		4				4			3	3				
A1.1	5		4				4			3	3				
A1.2	4		3				3			3	3				
A1.3	3		3				3			3	3				
A1.4	3		3				3			3	3				
A2	2		2				3			3	3				
A3	3		4				4			3	3				
A4	5		5				4			3	3				
A5	4		4				3			3	3				
A6	4	3													
A7	4	3													
A8	3	2													
A9	4	3													
A10	3	2													
A11	2	2													

Tabulka 7: Zranitelnost, ohodnocení

Aktiva	Hrozby	H1 3	H2 4	H3 4	H4 4	H5 5	H6 3	H7 3	H8 3	H9 4	H10 3	H11 5	H12 3	H13 3	H14 1
A12	5		5		3	4				3	4				
A12.1	4		3			4				3	4				
A12.2	4		4		3	4				3	4				
A12.3	5		5		3					3	4				
A13	4				3										
A13.1	4				3										
A13.2	4				3										
A13.3	1				3										
A13.4	2				3										
A14	5		3		3										
A15	5	4	5	5	3							3			
A16	5	4	5	5	3							3			
A17	3	3	4	3	3							3			
A18	4		4	4	3							3			
A19	3				3					2	3		3		
A20	3				3					2	3		3		
A21	3									2	3		3		
A22	5			5				5	5				5	5	1
A23	5			5				4	4				4	4	1

Tabulka 8: Zranitelnost, ohodnocení - pokračování

Riziko

Výslednou matici míry rizika sestavíme z předchozí matice jednoduchým výpočtem.

Riziko = Aktivum * Hrozba * Zranitelnost

Na závěr fáze analýzy rizik stanovíme hranice pro vyznačení úrovně rizik.
Nejnižší možné riziko je 1 pro ohodnocení aktiva, hrozby i zranitelnosti číslem 1 (R1=1*1*1).
Nejvyšší možné riziko 125 nastává při ohodnocení aktiva, hrozby i zranitelnosti číslem 5 (R5=5*5*5).

Úroveň 1, rozsah : 1-45
popis : nízká míra rizika - riziko je přijatelné a není potřeba je snižovat

Úroveň 2, rozsah 46-85
popis : střední míra rizika - riziko je potřeba snížit nebo eliminovat přijmutím preventivních opatření

Úroveň 3, rozsah 86-125
popis : kritická míra rizika - naléhavá pořeba stanovit ochranná opatření a vypracovat scénáře obnovy poškozených aktiv

Aktiva	Hrozby	H1 3	H2 4	H3 4	H4 4	H5 5	H6 3	H7 3	H8 3	H9 4	H10 3	H11 5	H12 3	H13 3	H14 1
A1	5		80				60			60	45				
A1.1	5		80				60			60	45				
A1.2	4		48				36			48	36				
A1.3	3		36				27			36	27				
A1.4	3		36				27			36	27				
A2	2		16				18			24	18				
A3	3		48				36			36	27				
A4	5		100				60			60	45				
A5	4		64				36			48	36				
A6	4	36													
A7	4	36													
A8	3	18													
A9	4	36													
A10	3	12													
A11	2	12													
A12	5		100		60	100				60	60				
A12.1	4		48			100				48	48				
A12.2	4		64		48	100				48	48				
A12.3	5		100		60					60	60				
A13	4				48										
A13.1	4				48										
A13.2	4				48										
A13.3	1				12										
A13.4	2				24										
A14	5		60		60										
A15	5	60	100	100	60							75			
A16	5	60	100	100	60							75			
A17	3	27	48	36	36							45			
A18	4		64	64	48							60			
A19	3				36					24	27		18		
A20	3				36					24	27		18		
A21	3									24	27		18		
A22	5			100				75	75				75	75	5
A23	5			100				60	60				60	60	5

Tabulka 9: Riziko, výpočet

Vyhodnocení analýzy rizik

Vyhodnocení analýzy rizik má klíčový význam pro přijetí potřebných opatření, aby dodávka poštovních služeb splňovala jak nároky na dostupnost, kvalitu a bezpečnost dat, tak požadavky na rychlou obnovu systému v případě havárie.

Výši rizika elektronické pošty v modelové společnosti pozitivně ovlivňuje implementovaná infrastruktura Exchange serveru. Použité technologie clusteru serverových rolí a existence záložní lokality výrazně snižuje možná rizika. Z tohoto důvodu také nejvyšší možná míra rizika dosáhla hodnoty 100, nikoliv 125.

Číselné hodnoty mají význam pro stanovení míry rizika pouze v kontextu této analýzy. Oceňování aktiv poštovního systému společnosti, podílu hrozeb a úrovně zranitelnosti bylo založeno na pětibodových stupnicích a s ohledem na infrastrukturu Exchange serveru 2007.

Vyhodnocení ukazuje kritickou míru rizika pro datová aktiva poštovního serveru, pro clustery, jenž jsou hostiteli serverových rolí a pro dostupnost aktivní i pasivní lokality. Nejvýraznější hrozbou je porucha hardwaru, selhání síťových služeb a chyba uživatele.

Nyní navrhnu opatření pro zvýšení ochrany všech aktiv s kritickým rizikem a pro vybraná aktiva se střední mírou rizika. Aktiva, na které lze uplatnit stejné principy ochrany budou slučována. Opatření mohou eliminovat také nežádoucí působení dalších hrozeb.

1. riziko
aktivum : A22 Aktivní lokalita, A22 Pasivní lokalita
hrozba : H3 Selhání sítě, nedostupnost
úroveň : kritická
opatření : Zajištění připojení každé lokality alespoň dvěmi nezávislými poskytovateli, dvěmi nezávislými síťovými technologiemi (např. leased line, DSL, satelitní spojení), Vytvoření plánu DR a převzetí služeb provozuschopnou lokalitou

2. riziko
aktivum : A15 CCR cluster (Mailbox), A16 NLB cluster (CAS,HUB)
hrozba : H2 Selhání HW , H3 Selhání sítě, nedostupnost
úroveň : kritická
opatření : instalace duálních síťových cest, vytvoření scénáře obnovy

3. riziko
aktivum : A12 data Exchange serveru
hrozba : H2 Selhání HW , H5 Selhání uživatele
úroveň : kritická
opatření : nastavení retenčních politik, Sestavení plánu a zálohování dat, vytvoření scénáře obnovy, organizace školení uživatelů

4. riziko
aktivum : A14 Disková pole
hrozba : H2 Selhání HW
úroveň : kritická
opatření : použití redundantních řadičů diskového/SAN pole, duálních cest

5. riziko
aktivum : A1 Exchange server
hrozba : H2 Selhání HW
úroveň : střední
opatření : obstarání náhradních součástí nebo serveru, vytvoření scénáře zotavení

6. riziko
aktivum : A1 Exchange server, A14 Disková pole
hrozba : H6 Provozní selhání, H9 Vandalismus
úroveň : střední
opatření : pravidelné zálohování a servisní údržba, omezení přístupu, kamerový systém

7. riziko
aktivum : A12 data Exchange serveru
hrozba : H9 Vandalismus, H10 Krádež
úroveň : střední
opatření : pravidelné zálohování, autorizovaný přístup, zabezpečení dat

8. riziko
aktivum : A21 Aktivní lokalita, A22 Pasivní lokalita
hrozba : H7 Výpadek elektrické energie, H13 Blesk
úroveň : střední
opatření : vybavení lokalit záložními zdroji elektrické energie, pravidelné revize a testování záložních zdrojů

9. riziko
aktivum : A21 Aktivní lokalita, A22 Pasivní lokalita
hrozba : H8 Porucha klimatizace
úroveň : střední
opatření : nepřetržitý monitoring teploty a vlhkosti s automatickým hlásicím systémem

10. riziko
aktivum : A21 Aktivní lokalita, A22 Pasivní lokalita
hrozba : H12 Požár, H13 Blesk
úroveň : střední
opatření : instalace čidel pro detekci kouře a požáru, automatický hlásicí systém napojený na složky požární ochrany

5 Řízená obnova poštovního systému v modelové společnosti

V rámci vyhodnocení analýzy rizik společnosti bylo navrženo několik ochranných opatřní pro včasnou detekci hrozby a snížení míry rizika určitých aktiv.

Zajištění budov aktivní a pasivní lokality před výpadkem elektrické energie, poruchou klimatizace, vznikem požáru a dalších možných přírodních katastrof je v plné kompetenci vlastníka těchto objektů. Požadavky na úroveň zabezpečení prostor včetně provádění periodického testování a revizí systému jsou dány smluvním vztahem nájemce a pronajimatele.

Hlavní náplní této části práce je vytvoření plánu řízené obnovy poštovní Exchange v popsané modelové společnosti.

K tomu se váží nasledující úkoly :

1. vytvořit Plán Disaster recovery pro poštovní služby Exchange 2007
2. vytvořit Plán scénářů řízené obnovy
3. vytvořit Scénáře řízené obnovy poštovních služeb

Scénáře řízené obnovy po havárii jsou zaměřeny pouze na poškození a ztrátu aktiv poštovního systému Exchange Server 2007 a odpovídajících hrozeb, kterými jsou :

- ztráta nebo nedostupnost lokality
- ztráta nebo poškození CCR clusteru
- ztráta nebo poškození NLB clusteru
- ztráta nebo poškození fyzického serveru, který je členem clusteru
- ztráta nebo poškození dat Exchange serveru
    - položka mailboxu
    - mailbox
    - mailbox databáze

5.1 Plán zotavení poštovní služby MS Exchange 2007

1. Hlavní cíle plánu DR
   - snížení rizika přerušení dodávky poštovních služeb
   - snížení rizika ztráty dat
   - omezení rozsahu dopadu havárie systému nebo jeho částí
   - zvýšení schopnosti rychlého zotavení systému po havárii
   - zvýšení opory a znalostí zaměstnanců nutné k provádění obnovy

2. Kompetence
vlastník plánu DR : společnost, jméno, pozice, kontakt
sestavování a údržba plánu : jméno, pozice, kontakt
kontrolní činnost : jméno, pozice, kontakt
revize plánu a distribuce : jméno, pozice, kontakt

3. Iniciace plánu
K iniciaci plánu DR je oprávněn : jméno, pozice, kontakt

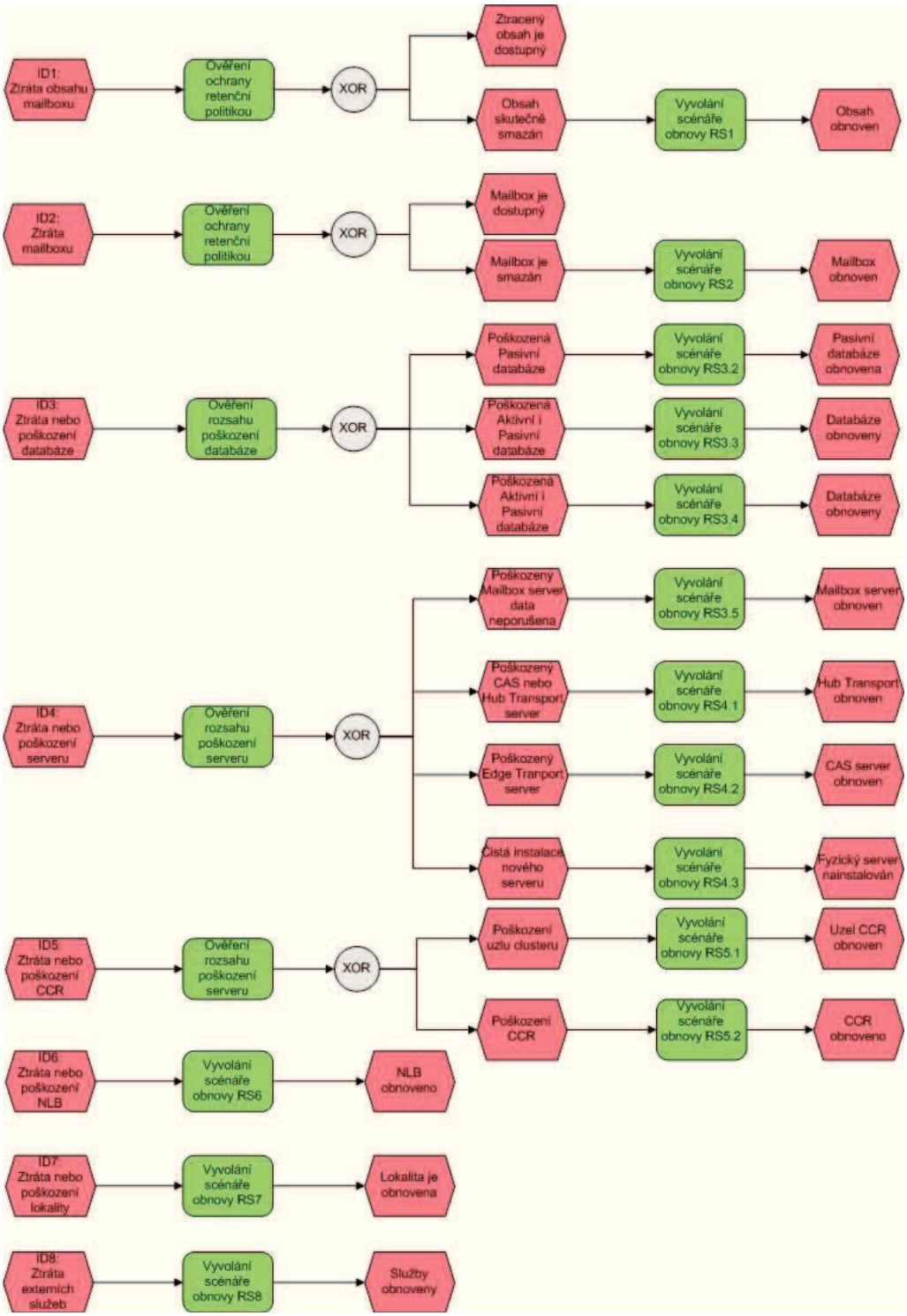
4. Seznam dokumentace a plánů
   - Dokument organizace společnosti
   - Dokument krizového řízení společnosti
   - Dokument infrastruktury Exchange serveru a fyzické lokace
   - Technická dokumentace (hw a sw požadavky, dodavatelé, servis)
   - Dokument konfigurace Exchange serveru
   - Dokument externích služeb Exchange serveru
   - Dokument umístění instalačních medií a datových záloh
   - Plány údržby systému
   - Plány zálohování a archivace dat
   - Plán scénářů řízené obnovy
   - Scénáře řízené obnovy poštovních služeb
   - Plán testování scénářů DR

5. Historie změn

Verze	Datum	Autor	Kontrola	Revize	Důvod změny

Tabulka 10: Historie změn

5.2 Plán scénářů řízené obnovy



Obrázek 7: Plán scénářů řízené obnovy

5.3 Scénáře řízené obnovy poštovních služeb

RS1: Obnova obsahu mailboxu
podmínky : retenční čas vypršel, obsah mailboxu nelze obnovit pomocí klienta
omezení: žádné
postup :
1. obnovit databázi do RSG viz RS3.1
2. zkontrolovat, příp.navýšit velikost stávajícího mailboxu
3. obnovit mailbox ze zálohy do složky „Restore“
`restore-mailbox -identity <UserName> -rsgdatabase <ServerName\ RSG_Name\DatabaseName> -TargetFolder 'Restore'`
4. zrušit databázi pro obnovu a RSG viz RS3.6

RS2 : Obnova mailboxu
podmínky : retenční čas vypršel, mailbox je definitivně smazaný
omezení: žádné
postup :
1. obnovit databázi do RSG viz RS3.1
2. vytvořit prázdný mailbox k uživatelskému účtu
3. zkontrolovat, příp.navýšit velikost nového mailboxu
4. obnovit mailbox ze zálohy do nového mailboxu
`restore-mailbox -identity <UserNname> -rsgdatabase <ServerName\ RSG_Name\DatabaseName>`
5. zrušit databázi pro obnovu a RSG viz RS3.6

RS3 : Obnova databáze

RS3.1 : Obnova databáze – do RSG
podmínky : žádné
omezení: žádné
postup :
1. vytvořit RSG
`new-storagegroup -Server<ServerName\ -LogFolderPath <path_to_Logfiles> -Name <RSG_Name> -SystemFolderPath \DatabasePath> -Recovery`
2. vytvořit novou databázi obnovy
`new-mailboxdatabase -mailboxdatabasetorecover <DatabaseName -storagegroup <Server\Name\RSG_Name> -EDBFilePath <DatabasePath>`
3. povolit přepis databáze zálohou
`set-mailboxdatabase -identity <ServerName\RSG_Name\DatabaseName> -AllowFileRestore:$True`
4. přihlásit se na zálohovací server, aplikace BE
5. vytvořit nový job : menu Job Setup > Restore Tasks > New Job

6. nastavit :
   - zdroj: Source > Selections (jméno výběru, server, SG/databáze, datum)
   - cíl: Destination > Microsoft Exchange Redirection (server, redirect to RSG)
   - job: Settings > General (jméno jobu, Overwrite the file on disk if it is older, Restore all information for files and directories)
7. spustit job: Run now
8. sledovat obnovu a vyčkat dokončení: menu Job Monitor
9. přimontovat obnovenou databázi na exchange serveru

```
mount-database -identity <ServerName\RSG_Name\DatabaseName>
```

RS3.2 : Obnova databáze – daty z aktivního uzlu „re-seed“
podmínky : poškozená databáze na pasivním uzlu, databáze na aktivním uzlu je neporušená
omezení: žádné
postup :
1. zastavit replikaci

```
Suspend-StorageGroupCopy-Identity: <ServerName\SG_Name>
```

2. odstranit soubor poškozené databáze (.edb), soubory logů (*.log) a kontrolní soubory (*.jrs, *.chk) v souborovém systému pasivního uzlu
3. obnovit pasivní databázi

```
Update-StorageGroupCopy-Identity: <ServerName\SG_Name>
```

RS3.3 : Obnova databáze – přepis stávající databáze
podmínky : poškozená databáze na pasivním i aktivním uzlu
omezení: po dobu obnovy jsou mailboxy nedostupné, délka obnovy závisí na velikosti databáze
postup :
1. povolit přepis poškozené databáze zálohou

```
set-mailboxdatabase -identity <ServerName\SG_Name\DatabaseName>
-AllowFileRestore:$True
```

2. odmontovat databázi

```
dismount-database -identity <ServerName\SG_Name\DatabaseName>
```

3. přihlásit se na zálohovací server, aplikace BE
4. vytvořit nový job : menu Job Setup > Restore Tasks > New Job
5. nastavit :
   - zdroj: Source > Selections (jméno výběru, server, SG/databáze, datum)
   - cíl: Destination > Microsoft Exchange Redirection (server, redirect to RSG)
   - job: Settings > General (jméno jobu, Restore over existing files, Restore all information for files and directories)
6. spustit job: Run now
7. sledovat obnovu a vyčkat dokončení: menu Job Monitor

8. přimontovat obnovenou databázi na exchange serveru
```
mount-database -identity <ServerName\SG_Name\DatabaseName>
```
9. odebrat povolení přepisu databáze
```
set-mailboxdatabase -identity <ServerName\SG_Name\DatabaseName>
-AllowFileRestore:$False
```
10. obnovit pasivní databázi - viz RS3.2

RS3.4 : Obnova databáze – přepis stávající databáze „Dial-tone“
podmínky : databáze je poškozena jak na pasivním tak i aktivním uzlu
omezení: po dobu obnovy jsou mailboxy použitelné, ale prázdné
postup :
1. odmontovat poškozenou databázi
```
dismount-database -identity <ServerName\SG_Name\DatabaseName>
```
2. v souborovém systému přesunout obsah složky se soubory databáze do jiného umístění pro případ pozdější obnovy, tak aby složka zůstala prázdná
3. vytvořit databázi dial-tone
```
mount-database -identity <ServerName\SG_Name\DatabaseName>
```
Pozn.:potvrdit kontrolní otázku, zda opravdu chceme vytvořit prázdnou databázi
4. poslat informativní mail uživatelům o vytvoření prázdných mailboxů
5. obnovit databázi do RSG viz RS3.1
6. výměna databáze viz RS3.7
7. sloučit data do aktivní databáze
```
Get-MailboxStatistics -database 'RSG_Name\DatabaseName'|restore-mailbox
```

RS3.5 : Obnova serveru – přenos databáze na jiný Exchange server s rolí mailbox „Database portability“
podmínky : původní mailbox server je poškozen, databáze je neporušená
omezení: po dobu obnovy jsou mailboxy nedostupné
postup :
1. vytvořit novou databáze na cílovém serveru
```
New-MailboxDatabase -StorageGroup <ServerName\SG_Name>
-Name <DatabaseName>
```
2. povolit přepis databáze
```
set-mailboxdatabase -identity <ServerName\SG_Name\DatabaseName>
-AllowFileRestore:$True
```
3. fyzický přesun databáze a potřebných souborů do cílové lokace (.edb, *.log, *.jrs, *.chk)
4. přimontovat přesunutou databázi na exchange serveru
```
mount-database -identity <ServerName\SG_Name\DatabaseName>
```

5. modifikovat lokaci mailboxů na všech uživatelských účtech staré databáze

```
Get-Mailbox -Database <SourceDatabase> |where $_.ObjectClass
-NotMatch '(SystemAttendantMailbox |ExOleDbSystemMailbox)'
|Move-Mailbox -ConfigurationOnly -TargetDatabase <TargetDatabase>
```

RS3.6 Zrušení databáze obnovy a RSG
postup :
1. odebrat databázi obnovy

```
Remove-MailboxDatabase -identity <ServerName\RSG_Name\DatabaseName>
```

2. odebrat RSG

```
Remove-Storagegroup -identity <ServerName\RSG_Name>
```

3. smazat vytvořená data z mista obnovy v souborovém systému

RS3.7 Výměna databáze - SWAP
postup :
1. odmontovat obě databáze

```
dismount-database -identity <ServerName\SG_Name\DatabaseName>
dismount-database -identity <ServerName\RSG_Name\DatabaseName>
```

2. přejmenovat databázové soubory v RSG podle názvů souborů dial-tone databáze
3. v souborovém systému :
   - vytvořit podsložky TEMP v místě databázových souborů RSG a obnovované SG
   - přesunout soubory z RSG do podsložky TEMP v obnovované SG
   - přesunout soubory z obnovované SG do podsložky TEMP v RSG
   - přesunout soubory z TEMP obou lokací do nadřazených složek (SG a RSG)
4. povolit přepis databáze pro obě databáze

```
set-mailboxdatabase -identity <ServerName\SG_Name\DatabaseName>
-AllowFileRestore:$True
set-mailboxdatabase -identity <ServerName\RSG_Name\DatabaseName>
-AllowFileRestore:$True
```

5. přimontovat obě databáze

```
mount-database -identity <ServerName\SG_Name\DatabaseName>
mount-database -identity <ServerName\RSG_Name\DatabaseName>
```

RS4 : Obnova serveru

RS4.1 : Obnova serveru – role Hub Transport nebo CAS
podmínky : AD je neporušeno
omezení: žádné
postup :

1. připravit server podle dokumentace :
   - technická dokumentace (hw a sw požadavky, dodavatelé, servis)
   - dokument konfigurace Exchange serveru
2. spustit obnovu z AD

```
setup / m:RecoverServer
```

3. při obnově role CAS, obnovit konfiguraci IIS

```
restorevdir.ps1 owa.xml
```

RS4.2 : Obnova serveru – role Edge Transport
podmínky : žádné
omezení: žádné
postup :
1. připravit a nainstalovat server podle dokumentace :
   - technická dokumentace (hw a sw požadavky, dodavatelé, servis)
   - dokument konfigurace Exchange serveru
2. obnovit konfiguraci

```
ImportEdgeConfig.ps1 edge.xml
```

RS4.3 : Obnova serveru – čistá instalace
podmínky : AD je neporušeno
omezení: žádné
postup :
1. připravit a nainstalovat server podle dokumentace :
   - technická dokumentace (hw a sw požadavky, dodavatelé, servis)
   - dokument konfigurace Exchange serveru

RS5 : Obnova CCR

RS5.1 : Obnova CCR – uzel clusteru
podmínky : jeden uzel je funkční
omezení: žádné
postup :
1. nastavit nepoškozený uzel jako aktivní
2. odebrat poškozený uzel ze Správce clusteru
3. připravit server podle dokumentace:
   - technická dokumentace (hw a sw požadavky, dodavatelé, servis)
   - dokument konfigurace Exchange serveru
4. přidat nový server do clusteru
5. nainstalovat pasivní uzel Exchange 2007
6. obnovit pasivní databázi viz. RS3.2

RS5.2 : Obnova CCR – celý cluster
podmínky : AD je neporušeno
omezení: žádné
postup :
1. vytvořit nový CCR cluster a MNS quorum na serverech odpovídajících parametrů podle dokumentu konfigurace Exchange serveru
2. nainstalovat pasivní Mailbox role na první obnovovaný uzel
3. obnovit serverové nastavení z AD
`Setup.com /recoverCMS /CMSName:<name> /CMSIPaddress:<ip>`
4. obnovení databáze za použití některého ze scénářů RS3.3, RS3.4 nebo RS3.5
5. přidání dalšího (pasivního) uzlu clusteru
6. obnovení databáze z aktivního uzlu viz. RS3.2

RS6 : Obnova NLB
podmínky : AD je neporušeno
omezení: žádné
postup :
1. je-li poškozen člen clusteru, odebrat poškozený uzel ze Správce clusteru
2. je-li poškozen celý cluster, reinstalovat NLB cluster dle dokumentu konfigurace Exchange serveru
3. provést obnovu serveru viz RS4.1

RS7 : Obnova lokality
podmínky : žádné
omezení: žádné
postup :
1. převést všechny aktivní databáze do nepoškozené lokality
2. obnovit externí služby viz RS8
3. obnovit databáze z aktivního uzlu viz 3.2
4. byla-li obnovena aktivní lokalita, přesunout služby zpět do obnovené lokality

RS8 : Obnova externích služeb
podmínky : žádné
omezení: žádné
postup :
1. postupovat dle dokumentu externích služeb Exchange serveru

6 Testování

Hlavním cílem testování je prověřit, zda poštovní služby mohou být podle vypracovaných scénářů skutečně obnovené a délka obnovy nepřesáhne stanovenou dobu. Z tohoto důvodu je nutné každý nově sestavený scénář řízené obnovy před uvedením v platnost řádně otestovat ve vhodném prostředí.

Za vhodné je považováno testovací prostředí, které odpovídá podmínkám reálného prostředí společnosti. Vykonávat tzv. ostré testy v reálném prostředí se zvláště pro nové scénáře nedoporučuje, jelikož scénář může vykazovat chyby a způsobit tak skutečný pád systému nebo ztrátu cenných dat.

Testování by měli provádět členové týmu obnovy, kteří v případě havárie budou obnovu poštovních služeb skutečně vykonávat. Průběh testu, výsledky i případné nejasnosti je nutné důsledně dokumentovat, neboť provedené záznamy se dále analyzují a vyhodnocují. Jsou–li zjištěny jakékoli nedostatky ve scénáři obnovy musí se iniciovat změnové řízení a scénář opravit.

Před zahájením testování musí být vždy jasně definováno co bude předmětem testování, z jakého důvodu se testování provádí, kdo bude testování provádět, v jakém prostředí a který scénář obnovy bude použit. Předem musí být rovněž stanoven hodnotící systém, aby výsledky testu nebyly znehodnoceny následně uzpůsobenou klasifikací.

Předmětem testování může být kompletní plán obnovy, jednotlivé scénáře, aplikace, hardwarové prostředky, výkonnost záložních systémů, připravenost týmu obnovy nebo personálu, schopnost krizového řízení organizace, schopnost vyhledat potřebnou dokumentaci atd.

Za důvod lze považovat testování nového scénáře, opravu scénáře nebo změnu podmínek a pravidelné testy.

Testování mohou provádět členové týmu obnovy, ostatní personál nebo externí společnost.

U prostředí volíme nejčastěji mezi testováním "od stolu", prováděním testů v testovacím prostředí a ostrými testy. Zvolený typ prostředí ovlivňuje váhu testu, přičemž nejvyšší váhu představují ostré testy.

Hodnotící systém závísí na předmětu testování. Hodnotit lze dosažení stanoveného cíle, dostupnost zdrojů (datových záloh, dokumentace), délku obnovy nebo jednotlivých kroků scénáře, reakce personálu na nečekanou událost, atd.

Význam testování nesmí být podceňován. Vedle testování nových scénářů je nutné vykonávat testování v pravidelných či nepravidelných intervalech, avšak minimálně jedenkrát ročně. Samozřejmostí jsou revize plánu a testování po každé významné změně.

Výsledky testování je nutné analyzovat a v případě neúspěchu vyvodit patřičné důsledky a přijmout nápravná opatření. Ta mohou představovat změnu scénáře, zvýšení povědomí personálu, ale také optimalizaci prostředí nebo zvýšení zabezpečení.

6.1 Testování scénářů řízené obnovy

Testování scénářů řízené obnovy bude probíhat shodně pro všechny vytvořené scénáře. Předmětem testování budou tedy jednotlivé scénáře obnovy poštovního systému. Důvodem je testování nově vytvořených scénářů. Proto bude testování probíhat v připraveném testovacím prostředí.

Vlastní testování bude zaměřeno na na následující vlastnosti :

1. správnost (3 body)
Je požadovaná obnova podle scénáře proveditelná?

2. srozumitelnost (2 body)
Je scénář dostatečně srozumitelný a přehledný ?

3. čas obnovy (5 bodů)
Je obnova provedena v očekávaném čase (dodržení RTO) ?

4. ztráta dat (5 bodů)
Byla obnova provedena bez, příp. s minimální ztrátou dat (dodržení RPO) ?

5. splnitelnost (5 bodů)
Byl splněn hlavní cíl testu ?

Hodnotící systém

Hodnotící systém jednotlivých testů je založen na hodnocení výše uvedených vlastností. Za kladné odpovědi je připočítán odpovídající počet bodů. Výsledný součet pak ukazuje úspěšnost testu.

Výsledné hodnocení :
Úroveň 1, rozsah : 0 - 8 bodů
neúspěšné testování, scénář je nutné urychleně přepracovat

Úroveň 2, rozsah : 9 - 14 bodů
průměrné testování, doporučení hlubší analýzy výsledků a přijmutí opatření

Úroveň 3, rozsah :15 - 20 bodů
úspěšné testování, scénář není nutné měnit

	1.	2.	3.	4.	5.	poznámka	celkem
RS1	3	2	5	5	5	závislost RS3.1, RS3.6	20
RS2	3	2	5	5	5	závislost RS3.1, RS3.6	20
RS3.1	3	2	5		5	závislost RPO na použitelnosti záloh	15
RS3.2	3	2	5	5	5		20
RS3.3	3	2	5		5	závislost RS3.2 RPO na použitelnosti záloh	15
RS3.4	3	-	5		5	závislost RS3.1, RS3.7, RS3.6 RPO na použitelnosti záloh příliš přeskakování mezi scénáři	13
RS3.5	3	2	5	5	5		20
RS3.6	3	2	5	5	5		20
RS3.7	3	-	5	5	-	chybí logická souslednost	13
RS4.1	3	2	5	5	5		20
RS4.2	3	2	5	5	5		20
RS4.3	-	-	-	-	-	scénář není využíván ani odkazován	0
RS5.1	3		5	5	5	závislost RS3.2 nutná znalost práce s clusterem	18
RS5.2	3		5	5	5	závislost RS3.2 - RS3.5 nutná znalost práce s clusterem	18
RS6	3		5	5	5	závislost RS4.1 nutná znalost práce s clusterem	18
RS7	3	2	5	5	5	závislost na RS8, RS3.2	20
RS8	3	2		5		RTO a splnitelnost závisí na plánech obnovy externích služeb	10

Tabulka 11: Testování scénářů obnovy

6.2 Vyhodnocení testování

Vyhodnocení testů ukazuje , že do úrovně č.1 s nejmenším počtem bodů se zařadil scénář RS4.3. Tento scénář byl vytvořen jako základní pro instalaci serveru. Ale jelikož se ukázalo, že není využíván žádným jiným scénářem, neboť tato část je zachycena přímo v konkrétních scénářích, je tento scénář nadbytečný a bude zrušen.

Do úrovně č.2 s rozpětím 9 až 14 bodů se řadí scénáře RS3.4, RS3.7 a RS8.

- RS3.4 a RS3.7 - scénáře společně zachycují jednu událost obnovy. Jelikož RS3.7 není využíván jinými scénáři převedeme tuto část přímo do RS3.4. Spojením se vyřeší logická návaznost, omezí se přeskoky mezi scénáři a usnadní orientace při obnově.
- RS8 - nízké ohodnocení scénáře odpovídá jeho plné závislosti na plánech a schopnostech obnovy externích služeb. Scénář bude zachován, úpravy nejsou zapotřebí.

Ostatní scénáře obnovy dosáhly na stanovenou hranici alespoň 15 body a budou ponechány beze změn.

Oprava scénáře RS3.4

RS3.4 : Obnova databáze – přepis stávající databáze „Dial-tone“
podmínky : databáze je poškozena jak na pasivním tak i aktivním uzlu
omezení: po dobu obnovy jsou mailboxy použitelné, ale prázdné
postup :
1. poškozená databáze je odpojená, příp. databázi odpojíme

```
dismount-database -identity <ServerName\SG_Name\DatabaseName>
```

2. v souborovém systému přesunout obsah složky se soubory databáze do jiného umístění pro případ pozdější obnovy (složka zůstane prázdná)
3. vytvořit databázi dial-tone

```
mount-database -identity <ServerName\SG_Name\DatabaseName>
```

Pozn.:kontrolní otázka, zda opravdu chceme vytvořit prázdnou databázi
4. poslat informativní mail uživatelům o vytvoření prázdných mailboxů
5. obnova databáze – do RSG viz RS3.1
6. výměna databáze - SWAP
    1. odmontovat obě databáze

```
dismount-database -identity <ServerName\SG_Name\DatabaseName>
dismount-database -identity <ServerName\RSG_Name\DatabaseName>
```

    2. přejmenovat databázové soubory v RSG podle názvů databáze dial-tone
    3. v souborovém systému :
        - vytvořit podsložky TEMP v místě databázových souborů RSG a SG
        - přesunout soubory z RSG do podsložky TEMP v obnovované SG
        - přesunout soubory z obnovované SG do podsložky TEMP v RSG
        - přesunout soubory z TEMP do nadřazených složek (SG a RSG)
    4. povolit přepis databází zálohou pro obě databáze

```
set-mailboxdatabase -identity <ServerName\SG_Name\DatabaseName>
-AllowFileRestore:$True
set-mailboxdatabase -identity <ServerName\RSG_Name\DatabaseName>
-AllowFileRestore:$True
```

    5. přimontovat obě databáze

```
mount-database -identity <ServerName\SG_Name\DatabaseName>
mount-database -identity <ServerName\RSG_Name\DatabaseName>
```

7. sloučit data do aktivní databáze

```
Get-MailboxStatistics -database 'RSG_Name\DatabaseName'|restore-mailbox
```

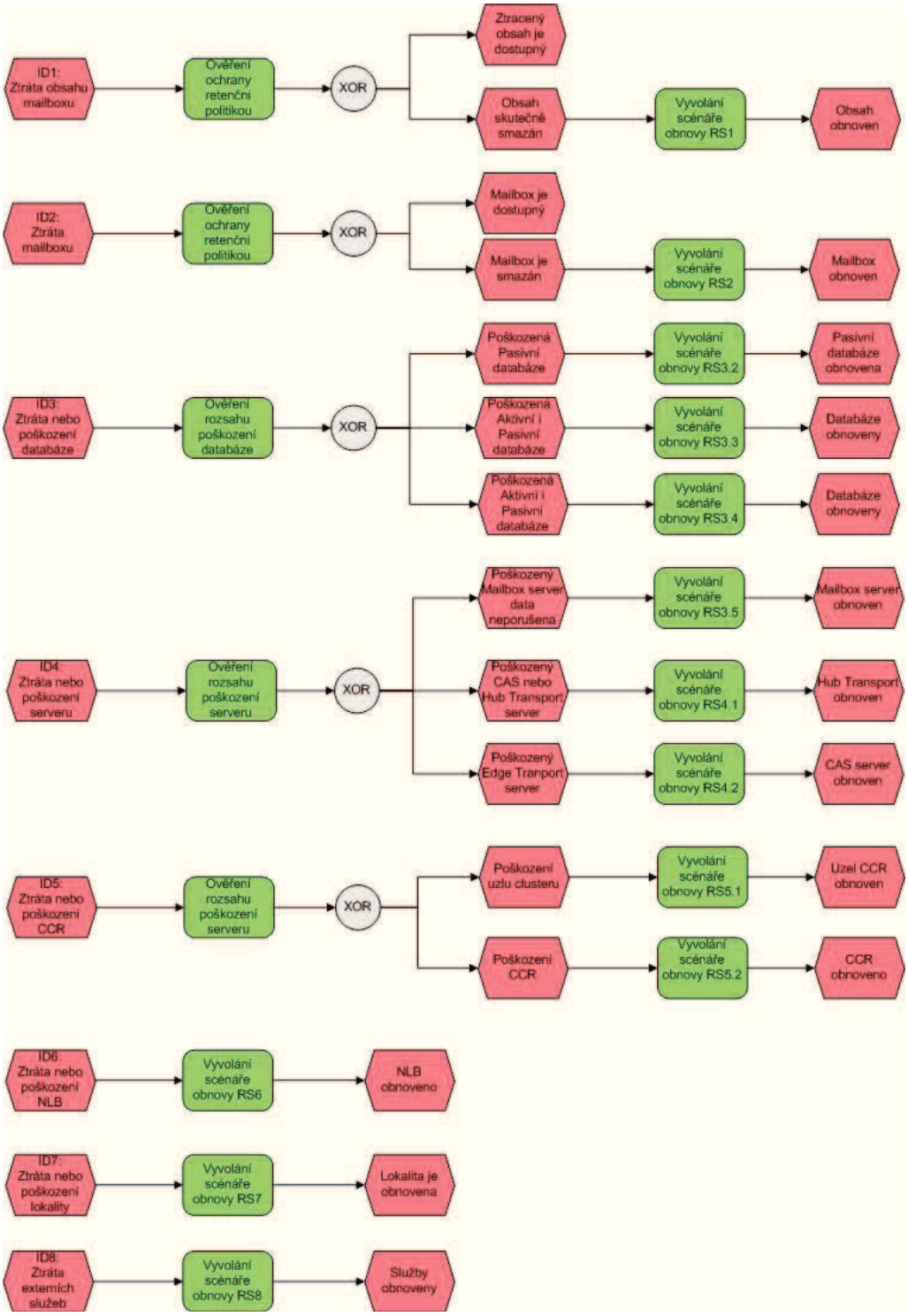
Nové testování scénáře RS3.4

	1.	2.	3.	4.	5.	poznámka	celkem
RS3.4	3	2	5		5	závislost RS3.1, RS3.6,RPO na použitelnosti záloh	15

Tabulka 12: Nové testování scénáře RS3.4

Opravený scénář dosáhl hodnocení 15 bodů a bude takto ponechán.

Na závěr zkontroluji vliv odstranění RS4.3 a RS3.7 na plán scénářů řízené obnovy.



Obrázek 8: Plán scénářů řízené obnovy - oprava

7 Závěr

Cílem diplomové práce bylo prostudování oblasti obnovy poštovních systémů a služeb na bázi Microsoft Exchange a podrobněji se seznámit s řízením kontinuity služeb v rámci procesů ITIL. Neboť metodika ITIL a její doporučení v oblasti procesního řízení IT je pro zajištění vysoké úrovně kvality a efektivity poskytovaných služeb implementována v řadě moderních společností.

V souvislosti s poštovním systém MS Exchange, jsou v práci zachycené nejen hrozby, které představují vysokou míru rizika pro zajištění kontinuity poskytování služeb, ale také možnosti snížení těchto rizik a kroky vedoucí k včasnému zotavení poštovních služeb.

V popsané modelové společnosti s implementovaným poštovním systémem Exchange 2007 jsou tato teoretická východiska využita k vytvoření analýzy rizik a sestavení jednotlivých scénářů obnovy poštovních služeb a dat.

V závěrečné části byly všechny vytvořené scénáře otestovány v připraveném prostředí. Po vyhodnocení testů a provedení optimalizace plánu obnovy jsou scénáře korektní a jsou připraveny k použití v dané společnosti.

Lenka Kučerová

8 Reference

[1] MERNA, Tony, AL-THANI, F., Faisal, *Risk management*,
1. vyd. BIZBOOKS 2007 , ISBN : 978-80-251-1547-3

[2] ČERMÁK, Miroslav, *Řízení informačních rizik v praxi* ,
1. vyd. Tribun EU 2009, ISBN : 978-80-7399-731-1

[3] CARTLIDGE, Alison, HANNA, Ashley, RUDD, Colin, MACFARLANE, Ivor,
WINDEBANK, John, RANCE, Stuart, *Úvodní přehled ITIL ® V3* ,
1. vyd. itSMF Czech Republic 2007, ISBN : 0-9551245-8-1

[4] TAYLOR, Sharon a tým autorů ITIL, *ITIL Service Design* ,
1. vyd. The Stationery Office 2007, ISBN : 978-01-133-1047-0

[5] *Disaster Recovery* [online], c2010 [cit.2012-02-02].
Dostupné z: < http://technet.microsoft.com/cs-cz/>

[6] *ITIL* [online], c2007 [cit.2012-02-02].
Dostupné z: < http://ITIL.cz/>

[7] *Disaster-resource* [online], c2005 [cit.2012-02-02].
Dostupné z: < http://www.disaster-resource.com/>

[8] *ISO/IEC 20000* [online], c2011 [cit.2012-02-02].
Dostupné z: < http://www.iso.org/>

[9] *ISO/IEC 27001* [online], c2011 [cit.2012-02-02].
Dostupné z: < http://www.iso.org/>

A Typický obsah plánu obnovy

Stručný popis plánu obnovy dle doporučení ITIL a části, které by měl obsahovat.

A.1 Dokumentace

Dokumentace musí být udržována tak, aby systémy, infrastruktura a zařízení splňovaly požadavky na obnovu podnikání.

A.1.1 Distribuce dokumentů

Distribuce dokumentů se řídí dle následujícího rozdělovníku :

kopie	jméno	datum předání	pozice
1.			
2.			
3.			
4.			

Tabulka 13: Distribuce dokumentů

A.1.2 Revize dokumentů

Dokument bude revidován každých X měsíců.
Aktuální revize: datum
Další revize: datum

Záznam o provedených revizích, verzích plánu obnovy a přehled změn:

datum revize	č.verze	přehled změn

Tabulka 14: Revize dokumentů

A.1.3 Schválení dokumentů

Seznam osob oprávněných ke schvalování dokumentů je zahrnut v tabulce č.15.

jméno	pozice	podpis

Tabulka 15: Schválení dokumentů

A.2 Podpůrné informace

A.2.1 Úvod

Dokument zahrnuje pokyny a postupy, které je třeba dodržovat při obnově systémů, infrastruktury, služeb a zařízení nebo při udržení kontinuity služeb na stanovené úrovni.

A.2.2 Strategie obnovy

Systémy, infrastruktura, služby nebo zařízení budou obnoveny do alternativních systémů, infrastruktury, služeb nebo zařízení. Obnovení systémů, infrastruktury, služeb nebo zařízení bude trvat přibližně X hodin. Systém bude navrácen do posledního známého bodu stability systému a integrity dat, který je vzdálený maximálně X hodin.

Požadovaná doba zotavení pro systém, infrastrukturu, služby nebo zařízení je:

Zotavení systému, infrastruktury, služeb nebo zařízení bylo naposledy testováno :

A.2.3 Vyvolání

Seznam pracovníků, kteří jsou oprávnění k vyvolání plánu obnovy:

1.
2.

A.2.4 Rozhraní a závislosti na jiných plánech

Podrobný popis vzájemných závislostí na ostatních plánech kontinuity podnikání.

A.2.5 Všeobecné pokyny

Postup pro předávání informací a komunikaci s veřejnými médii :

- zachovat klid a vyhnout se zdlouhavé konverzaci
- požadovat předložení žádosti o informace a eskalace této žádosti
- požádat o trpělivost (nesdělovat podrobnosti pokud to není nezbytně nutné)

- pokud kontaktujeme osoby, které drží pohotovost :
  - hovoříme-li s neoprávněnou osobou, požádat o kontakt na osobu oprávněnou
  - nelze-li kontaktovat, zanechat zprávu s žádostí o zavolání
  - nezanechávat podrobnosti o incidentu
  - vždy dokumentovat kdo byl kontatkován, průběh hovoru a následné akce

Všechny aktivity, kontaktování osob a eskalace incidentu by měly být jasně a přesně zaznamenány. Pro usnadnění by se měl použít kontrolní seznam se záznamem činností, kdo je prováděl, kdy byly zahájené a kdy ukončené.

A.2.6 Závislosti

Systém, infrastruktura, služby, zařízení nebo rozhraní, které je potřeba využít ve spojení s plánem obnovy, musí být zdokumentovány (podle pořadí priorit) tak, aby v případě potřeby mohly být snadno identifikovány a připraveny příp. obnoveny. Osoba odpovědná za vyvolání by měla zajistit koordinaci aktivit s dalšími plány obnovy.

systém	odkaz na dokument	kontakt

Tabulka 16: Závislosti

A.2.7 Seznam kontaktů

Seznamy všech důležitých osob, organizací a kontaktních údajů :

jméno	organizace / útvar	pozice	kontakt

Tabulka 17: Seznam kontaktů

A.2.8 Tým obnovy

Osoby zodpovědné za provádění nebo zajišťění vykonávání obnovy a dokumentaci problémů, které se vyskytnou. Kontaktování týmu obnovy se provádí pomocí běžných postupů eskalace.

jméno	pozice	kontakt

Tabulka 18: Tým obnovy

A.2.9 Kontrolní seznam

Pro snazší orientaci a včasné provádění klíčových činností se využívá kontrolní seznam:

úkol	cílový stav	aktuální stav
potvrdit vyvolání		
iniciovat strom volání a eskalační procedury		
spolupracovat s dalšími plány obnovy		
zajistit odeslání zálohovacích médií a dokumentace do místa obnovy		
mobilizovat tým obnovy		
zahájit akce obnovy		
kontrolovat průběh obnovy		
informovat tým obnovy o hlášených požadavcích		
kontrolovat požadavky se všemi tými obnovy		
komunikovat se zákazníky a řídit dokončení obnovy		

Tabulka 19: Kontrolní seznam